(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 734 556 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
04.09.2002 Bulletin 2002/36

(21) Application number: **95905366.1**

(22) Date of filing: **13.12.1994**

(51) Int Cl.[7]: **G07F 7/10**

(86) International application number:
PCT/US94/14319

(87) International publication number:
WO 95/016971 (22.06.1995 Gazette 1995/26)

(54) NETWORK BASED PAYMENT SYSTEM AND METHOD FOR USING SUCH SYSTEM

DATENNETZGESTÜTZTES ZAHLUNGSSYSTEM UND VERFAHREN ZUM GEBRAUCH EINES DERARTIGEN SYSTEMS

SYSTEME DE PAIEMENT BASE SUR UN RESEAU DE DONNE ET METHODE POUR L'UTILISATION D'UN TEL SYSTEME

(84) Designated Contracting States:
BE DE FR GB IT NL

(30) Priority: **16.12.1993 US 168519**

(43) Date of publication of application:
02.10.1996 Bulletin 1996/40

(60) Divisional application:
02007486.0 / 1 235 177

(73) Proprietor: **Open Market, Inc.**
Cambridge, MA 02141 (US)

(72) Inventor: **GIFFORD, David, K.**
Weston, MA 02193 (US)

(74) Representative: **Blatchford, William Michael et al**
Withers & Rogers
Goldings House,
2 Hays Lane
London SE1 2HW (GB)

(56) References cited:
US-A- 4 775 935
US-A- 4 799 156
US-A- 4 812 628
US-A- 4 922 521
US-A- 4 935 870
US-A- 4 992 940
US-A- 5 025 373

EP 0 734 556 B1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The recent rapid growth of information applications on international public packet-switched computer networks such as the Internet suggests that public computer networks have the potential to establish a new kind of open marketplace for goods and services. Such a marketplace could be created with a network sales system that comprises a plurality of buyer and merchant computers, means for the users of the buyer computers to display digital advertisements from the merchant computers, and means for the users to purchase products described by the advertisements.

[0002] A network based sales system will need to allow users to preview products at little or no cost, and will need to make a large number of product advertisements available in a convenient manner. In addition, the shopping system will need to include easy-to-use facilities for a user to purchase desired products using a merchant independent payment method. In addition the network sales will need to allow new buyers and merchants to enter the market.

[0003] A central requirement for a marketplace is a payment mechanism, but at present no merchant independent payment mechanism is available for computer networks that permits users to utilize conventional financial instruments such as credit cards, debit cards, and demand deposit account balances. We expect that both retail payment and wholesale payment mechanisms will be required for networks, with consumers using the retail mechanism for modest size purchases, and institutions using the wholesale mechanism for performing settlement between trading partners. For wide acceptance the retail mechanism will need to be a logical evolution of existing credit-card, debit-card, and Automated Clearing House facilities, while for acceptance the wholesale mechanism will need to be an evolved version of corporate electronic funds transfer.

[0004] US 4,799,156 discloses a system for interactive on-line electronic communications and processing of business transactions between a plurality of different types of independent users including a plurality of sellers, and a plurality of buyers, as well as financial institutions. Using the system, a buyer is able to instruct its bank to pay a bill to a distributor or another financial institution.

[0005] US 5,025,373 discloses a portable personal banking system which utilizes an encryption algorithm to securely transmit data between a host bank computer and a personal banking terminal.

[0006] According to one aspect of the present invention, there is provided a network based payment system having the features of claim 1. According to another aspect of the invention, there is provided a method of using a network based payment system as recited in claim 8.

[0007] A preferred feature of the invention is to provide a network based payment system that will authorize payment orders and remove part of the risk of fraud from merchants.

[0008] An unavoidable property of public computer networks is that they are comprised of switching, transmission, and host computer components controlled by many individuals and organizations. Thus it is impossible for a network based payment system to depend upon a specified minimum required degree of software, hardware, and physical security for all of the components in a public network. For example, secret keys stored in a given user's personal computer can be compromised, switches can be tempered with to redirect traffic, and transmission facilities can be intercepted and manipulated.

[0009] The risk of performing retail payment in a public network is compounded by statutes that make a payment system operator in part liable for the security lapses of its users. Existing Federal statutes in the United States, including the Electronic Funds Transfer Act and the Consumer Credit Protection Act, require the operator of a payment mechanism to limit consumer liability in many cases. Payment system operators may have other fiduciary responsibilities for wholesale transactions. Similar responsibilities exist in other countries for retail and wholesale transactions.

[0010] In existing credit card payment systems, a credit card's issuing bank takes on the fraud risk associated with misuse of the card when a merchant follows established card acceptance protocols. Acceptance protocols can include verifying a card holder's signature on the back of their card and obtaining authorization for payments over a certain value. However, in network based commerce a merchant can not physically examine a purchasers credit card, and thus the fraud risk may revert to the merchant in so called "card not present" transactions. Many merchants can not qualify to take this risk because of their limited financial resources. Thus the invention is important to allow many merchants to participate in network based commerce.

[0011] Further preferred features of the invention include utilizing existing financial instruments such as credit cards, debit cards, and demand deposit accounts for merchant payments.

[0012] Existing network-based payment systems do not connect to the financial system for authorization and are not compatible with conventional financial instruments. Existing network based payment systems include the Simple Network Payment Protocol [Dukach, S., SNPP: A Simple Network Payment Protocol, MIT Laboratory for Computer Science, Cambridge, MA, 1993.], Sirbu's Internet Billing Server [Sirbu, M. A., Internet Billing Service Design and Prototype Implementation, Information Networking Program, Carnegie-Mellon University, 1993], and NetCash [Medvinsy, G., and Newman, B. C., NetCash: A Design for Practical Electronic Currency on the Internet, Proc. 1st ACM Conf. on Comp. and Comm. Security, November, 1993].

[0013] A further preferred feature of the invention is to allow users in an untrusted network environment to

use conventional financial instruments without requiring modification to existing financial system networks.

[0014] The following definitions apply to the present invention. A principal is a person, company, institution, or other entity that is authorized to transact business as part of a network payment system. A payment order describes the identity of a sender, a payment amount, a beneficiary, and a sender unique n-once. A sender is a principal making a payment. A beneficiary is a principal to be paid by the payment system. A sender unique nonce is an identifier that is used only once by a given sender. An example of sender unique nonces are unique timestamps. An external account is an account that can be used to settle a payment order for either a sender or a beneficiary in the external financial system. Examples of external accounts include demand deposit accounts and credit card accounts. An external device is a physical object that is kept in the possession of a user for the purpose of identifying the user.

[0015] A network based payment system is a service that authorizes and executes digital payment orders that are backed by external accounts. A payment system authenticates a payment order, checks for sufficient funds or credit, and then originates funds transfer transactions to carry out the payment order. A payment system acknowledges acceptance or rejection of a payment order. More than one payment system may exist on a given network, and a given payment system may operate on more than one host to increase its reliability, availability and performance. An authenticator is a digital value that is appended to a payment order and becomes part of the payment order that authenticates the payment order as genuine.

[0016] The invention will now be described, by way of example, with reference to the accompanying drawings in which:

Figure 1 is a block diagram of a typical network based sales system;
Figure 2 is a screen snapshot of a buyer computer display of an overview page from a merchant computer;
Figure 3 is a screen snapshot of a buyer computer display of a page of digital advertisements from a merchant computer;
Figure 4 is a screen snapshot of a buyer computer display of an account query page;
Figure 5 is a screen snapshot of a buyer computer display of a fulfillment page;
Figure 6 is a flow chart illustrating the processing of a sale between a buyer computer and a merchant computer;
Figure 7 is a flow chart illustrating the alternate processing of payment order means for obtaining missing payment information;
Figure 8 is a screen snapshot of a buyer computer display of an overview page from a merchant computer that contains a query input by the user;
Figure 9 is a screen snapshot of a buyer computer display of digital advertisements in response to a user's query;
Figure 10 is a screen snapshot of a buyer computer screen of a purchase confirmation;
Figure 11 is a screen snapshot of a buyer display of a fulfillment page like Figure 5;
Figure 12 is a flow chart illustrating an alternate processing of a sale between a buyer computer and a merchant computer where a payment order is pre-authorized;
Figure 13 is a block diagram of a typical network based payment system in accordance with the invention;
Figure 14 is a flow chart illustrating the authentication, authorization, and settlement of a payment order;
Figure 15 is a flow chart illustrating an alternate processing of the authentication and verification of a payment order where transaction identifiers are used; and
Figure 16 is a flow chart illustrating an alternate processing of the authorization of a payment order where real-time approval from the financial authorization network may not be obtained.

[0017] A network based sales system 200 as shown in Figure 1 employs a network 67 to interconnect a plurality of buyer computers 61 and 62, merchant computers 63 and 64, each merchant computer with respective digital advertisement databases 65 and 66, and a payment computer 68. A user of the system employs a buyer computer to retrieve advertisements from the merchant computers, and to purchase goods of interest. A payment computer is used to authorize a purchase transaction.

[0018] A digital advertisement includes a product description and a price. In digital advertisement database 65 prices and descriptions may be stored separately, and one price may apply to many product descriptions.

[0019] In an alternate embodiment, the network based sales system further includes external devices that are kept in the possession of users so that the users can authenticate themselves when they use a buyer computer.

[0020] The software architecture underlying the particular preferred embodiment is based upon the hypertext conventions of the World Wide Web. A document is defined to be any type of digital data broadly construed, such as multimedia documents that include text, audio, and video, and documents that contain programs.

[0021] Figure 2 shows an overview screen that has been retrieved from a merchant computer by a buyer computer and displayed by the buyer computer. It includes links 1, 2, and 3 that when activated by a user cause the buyer's computer to take specified actions. In the case of link 1, the document shown in Figure 3 is retrieved from a merchant computer and displayed. In

the case of link 2, a short audio segment is retrieved from a merchant computer and played. In the case of link 3, the query that can be entered into the query dialog box 4 is sent to a merchant computer, and a document is retrieved from the merchant computer and displayed.

[0022] Figure 3 shows a document that contains three digital advertisements. The digital advertisements have been retrieved from the merchant computer after the activation of link 1. The merchant computer may set the prices contained in the advertisements based on the the identity of the user as determined, for example, by the network address of the requesting buyer computer. The document includes links 5, 6, and 7 that are used to purchase the products described by the advertisements. For example, if link 5 is activated the missing payment information document shown in Figure 4 is retrieved from the merchant computer and displayed.

[0023] Figure 4 is a missing payment information document that is used to gather user account information for the requested purchase in an HTML form. Radio buttons 8, 9, 10, 11, 12 are used to select a means of payment, dialog box 13 is used to enter an account number, dialog box 14 is used to enter an optional authenticator for the account, purchase button 15 is used to send the account information to the merchant computer and proceed with the purchase, link 16 is used to abort the purchase and return to the document shown in Figure 2, and dialog box 17 is used to enter optional user information that is associated with the purchase and ultimately used by a financial institution as part of a textual billing identifier for the purchase transaction. If provided, this additional information is included in the payment order for the purchase.

[0024] Figure 5 is a fulfillment document 18 that is produced once valid account information is provided to the missing payment information document in Figure 4 and purchase button 15 is activated.

[0025] Figure 6 is a flowchart that more fully describes the information flow in the purchase transaction shown in Figures 2 to 5. An initial user inquiry 19 from activating link 1 results in the HTTP request 20 for a specific document with a specified URL. The URL specifies the name of the merchant computer. The merchant computer retrieves the document given the URL at 21, and returns it to the buyer computer at 22. The buyer computer displays the resulting HTML document at 23. When the user activates link 5, an HTTP request 25 is sent to the merchant computer requesting the document.

[0026] In an alternate embodiment, document 22 is executed at 23 as a program. A program is defined as a set of instructions that can exhibit conditional behavior based upon user actions or the environment of the buyer computer. As is known to those skilled in the art, there are many techniques for representing programs as data. The program can be interpreted or it can be directly executed by the buyer computer. The program when executed will cause the buyer computer to interact with the user leading to the user purchase request 24, and the purchase message 25.

[0027] The merchant computer then attempts to construct a payment order at 26 using the information it has gathered about the user. The buyer computer may have previously supplied certain credentials using fill out forms or other account identification means such as providing the network address of the buyer computer in the normal course of communication. If the merchant computer is able to construct a complete payment order at 26 the payment order is sent to a payment computer for authorization at 27. If a payment order can be constructed, processing continues at 28.

[0028] Alternatively, the buyer computer may construct the payment order at 24 and send it to the merchant computer at 25. In this case, the payment order assembly steps at 26, at the merchant computer, may only need to forward the payment order from the buyer computer.

[0029] A payment order includes user account information, merchant account information, an amount, and a nonce identifier that has not been previously used for the same user account. Variations of payment orders can be constructed, including payment orders that specify user or merchant identifiers in place of account information, payment orders that specify a valid time period, payment orders that specify foreign currencies, and payment orders that include comment strings. Part of the process of constructing a payment order is creating a corresponding authenticator using one of the authenticator methods described below.

[0030] In the illustrated embodiment of Figures 3 and 4, the merchant computer does not have sufficient information to construct a payment order at 26 and thus at 33 (Figure 7) constructs and returns a missing payment information document in response to request 25. Operation 33 includes in the constructed document appropriate form fields based on what information the merchant computer has already collected from the user. The document is returned to the buyer computer at 34 and is displayed at 35. When the user presses the purchase button 15, the contents of the form are transmitted to the merchant computer, at 36, to a specific URL name, using an HTTP request. Based on the supplied form fields, the merchant computer constructs a complete payment order. Alternatively, the buyer computer may construct the payment order at 35 and send it to the merchant computer as part of step 36. In this case, the payment order assembly steps 37 at the merchant computer simply passes on the payment order from the buyer computer. The payment order is sent to the payment computer in a message at 38.

[0031] In either case, the flowchart continues in Figure 6 where the payment computer checks the authorization of the payment order at 28. If the payment system authorizes the request, an authorization message at 29 is returned to the merchant computer, and the merchant computer checks at 30 that the authorization message came from the payment computer using the authentica-

tor mechanism described below. Assuming that the authorization message is valid, the merchant computer performs fulfillment at 30, returning the purchased product in response at 31. In our example in Figure 5 the response at 31 is document 18 that was the logical target of link 5. If the payment system does not authorize the payment order then response 31 is a rejection of the user's purchase request.

[0032] In an alternate embodiment, step 30 can encrypt the document using a key that is known to the buyer computer. As is known to those skilled in the art, the key can be communicated to the merchant computer using convention key distribution protocols. In this manner the document will be protected from disclosure to other users.

[0033] The fulfillment step at 30 can alternatively schedule a physical product to be shipped via ordinary mail or other means. This can be accomplished by updating a fulfillment request database or by sending a message to a shipping system. In this case the response at 31 is a confirmation that the product has been scheduled to ship. In this way the network sales system can implement an electronic mail order system.

[0034] Figures 8, 9, 10, and 11 show a second example that uses query based access to digital advertisements. It is assumed that the previous example was used by the user immediately before at the same buyer computer.

[0035] Figure 8 shows the overview screen where the query "movie review" has been entered into dialog box 39. When the user activates process button 40, the merchant searches databases as described by the URL attached to button 40, and creates a response document as shown in Figure 9.

[0036] Figure 9 shows digital advertisements 39, 40, 41, 42, 43, and 44 that were found in response to the query initiated by button 40. A scroll bar 45 shows that there are additional digital advertisements that are not shown. When link 46 is activated, the missing account information document shown in Figure 10 is returned by the merchant computer.

[0037] Figure 10 shows that the merchant computer has partial information on the buyer's account. Message 47 shows that the merchant computer already knows the buyer's account number. Purchase button 48 will send the optional user reference string in dialog box 50 to the merchant computer described by the URL behind button 48 and purchase the product corresponding to digital advertisement 39. Cancel link 49 will return the user to the document shown in Figure 2.

[0038] When purchase button 48 is activated, a document 51 is sent by the merchant computer and displayed by the buyer computer as shown in Figure 11.

[0039] Figure 12 shows an alternative method of processing a sales transaction. In this method when the user requests a purchase at 52, the buyer computer constructs a payment order at 53 and sends it for approval to the payment computer at 54. The payment computer authorizes the payment order at 55; and when the payment order is authorized, returns an unforgable certificate at 56 that the payment order is valid. Means of creating such unforgable certificates are described in authenticator method number one below. If at step 55 the payment order is not authorized, a rejection message is sent at 56 and the sales transaction is terminated.

[0040] The buyer computer then proceeds at 57 to send a pre-authorized purchase request to the merchant computer. The unforgable certificate 56 is included in a purchase message at 57 that is sent at 58 to the merchant computer. Based upon the pre-authorized payment order the merchant computer performs fulfillment at 59 and returns the product at 60. In a variation, the merchant computer at 59 checks to ensure the payment order has not been previously used. This can be accomplished by checking with a payment computer or maintaining a merchant computer database of previously accepted payment orders. The unforgable certificate created at step 56 does not need to include the user account information. This variation is useful if the user wishes to make purchases and remain anonymous to the merchant.

A Network Based Payment System

[0041] A network based payment system 300 as shown in Figure 13, employs a public packet-switched network 69 to interconnect a plurality of client computers 70 and 71, and a plurality of payment computers such as 72, each payment computer having an account database 73, a settlement database 74, an authorized address database 75, a sender credential database 76, a financial system interface 77, and a real-time authorization interface 78. The interfaces 77 and 78 may be implemented by a single communications line.

[0042] In an alternate embodiment, the network based payment system further includes external devices that are kept in the possession of users so that the users can authenticate themselves when they use a buyer computer.

[0043] Account database 73 maintains temporal spending amounts, such as the amount spent in the current day, and also maintains temporal spending limits. The account database may also maintain a translation between principal identifiers and external account identifiers. Settlement database 74 records committed payment orders along with any authorization information for the orders that was obtained from interface 78. Address database 75 maintains for each sender a list of authorized buyer computer and delivery addresses. Credential database 76 maintains a list of credentials for principals and information that can be used to authenticate principals.

[0044] Figure 14 is a flowchart that describes the operation of the payment system. A client computer 71 constructs a payment order at 79, and computes and

adds an authenticator to the payment order at 80. The payment order is sent at 81 to a payment computer, where the authenticator is verified at 82 to ensure that the payment order was originated by the sender it describes. Below we present different means of implementing 80 and 82.

[0045] If the payment order is authentic and address restrictions are desired, at 83, either or both of the client computer address or the specified delivery address can be checked against address database 75. If address restrictions are desired and if the addresses in the payment order are not in the database, the payment computer sends a rejection message to the client computer. Address database 75 specifies, for each principal, acceptable client computer addresses and delivery addresses. A delivery address can be a network address, or a street address for packaged goods. As is known in the art, database 75 can include wild-card specifications and similar techniques to reduce its size.

[0046] For example, database 75 could contain an entry for principal identifier "*@acme.com" restricting legal delivery addresses to "computer: *.com", "computer: cmu.edu", and "surface: *, 34 Main Street, Anytown, USA", indicating that any user at the company Acme can order products to be delivered to the network address at Acme or the university CMU, or to anyone at 34 Main Street, Anytown, USA.

[0047] If payment order address restrictions are not desired or have been checked, processing continues at 84 where the payment order is checked for replay and temporal spending limits. Replay is checked for by making sure that the sender did not previously present a payment order with the same nonce by checking an index of committed payment orders by nonce in settlement database 74. If nonces are based on time, then a payment order that is older than an administratively determined value can be rejected out of hand. Time based nonces or sequential nonces permit old nonces to be removed from the settlement database 74. If a payment order has been previously processed or its nonce is too old, the payment order computer sends a rejection message to the client.

[0048] After the payment order passes the replay check, temporal spending limits are checked in account database 73. These spending limits can be applied on a per sender, per group of senders, and per payment system basis to limit fraud risk. The limits can be applied to any duration of time, for example a maximum spending amount per hour or per day. If the payment order would violate a spending limit, the payment computer sends a rejection message to the client.

[0049] Once the payment order passes the temporal spending check at 84, a message is constructed at 85 to check that the external account that backs the sender's payment system account has adequate funds or credit. If the sender identifier in the payment order is not already an account number in the external financial system, it is translated into a corresponding account number in the external financial system using account database 73. A real-time authorization request message is sent at 86 to the external financial system over interface 78. If the external financial system approves authorization request 86, an authorization message is returned at 87. If request 86 is not approved, the payment computer sends a rejection message to the client at 87.

[0050] In a variation of the above described approach, processing continues at 95 after 84. At 95 real-time authorization is only obtained when the total of a sender's payments since the last real-time authorization reaches a preset value, or the payment order is over a preset amount. These preset values can be optionally recorded on a per principal basis in database 73 or can be administratively determined for all principals. In this manner, the number of messages to the external financial system can be reduced. In addition, the payment system can avoid making real-time authorization requests for small payments when the risk is acceptable to the payment system operator. If real-time authorization is necessary, processing continues at 85 after 95. If real-time authorization is not necessary for a request, at 100 the payment order amount is added to the sender's total of payments since the last real-time authorization in database 73, and processing continues at 88.

[0051] In another variation after 100 a check is made at 101 in database 73 to see if a background authorization process should be scheduled. A background authorization process permits the payment computer to continue its normal processing while it checks with the financial authorization network on the sender's account. This mechanism can be used to limit payment system risk. If the background authorization fails, the account is suspended by so updating database 73. If the sender's total of payments since last authorization is over a preset value stored in 73 then a background authorization process is scheduled at 102. Otherwise processing continues at 88.

[0052] In another variation, at 95 and 101 authorizations are obtained based on the amount spent since last authorization and time since last authorization.

[0053] At 88 the payment order is committed to execution and is recorded in settlement database 74. Recorded with the payment order in database 74 are portions of authentication message 87 that show that the payment computer contacted the remote financial system. The amount of the payment order is added to running temporal spending records in database 73, and an authorization message is sent to the client computer at 90. The authorization message includes the payment order. In an alternate embodiment, at 90 the authorization message contains a truncated payment order that includes at least the payment order's sender and the payment order's unique nonce.

[0054] In an alternate embodiment, the authorization message sent to the client at 90 includes at least one legal delivery address for the sender as determined from

database 75.

[0055] Authorization message 90 must be transmitted in such a way that the client computer can be sure that it came from the payment computer. At 89 a payment system specific authenticator is added to the payment order. At 91 this authenticator is checked by the client computer. The steps at 89 are a dual of step 80, and the steps at 91 are a dual of step 82. The authentication means for steps 89 and 91 are described below.

[0056] Finally, settlement is performed at 92 in the external financial system 77 between external accounts that correspond to the sender and the beneficiary. If settlement is accomplished as part of real-time authorization at steps 86 and 87, as may occur in a real-time debit network, then no other steps need to be taken. If settlement is not accomplished as part of the authorization process, then financial system messages are sent to interface 77 to effect settlement. Depending on the external accounts involved, these messages may include electronic funds transfer messages or automated clearinghouse messages.

[0057] In an alternate embodiment, at 92 settlement messages are sent to reconcile net transfer balances between principles on a temporal basis, for example once a day. In this embodiment the number of settlement messages can be less than the number of payment orders.

[0058] According to claims 1 and 8, authenticators are created and checked using one of the following first, second or third methods.

[0059] Fourth, fifth, sixth and seventh methods are also disclosed, which can be used by the payment computer and the client computer additionally in combination with any of the first, second and third methods.

[0060] In a first method for authenticators, at steps 80 or 89, a digest of the payment order is signed by the sending computer using a public-key cryptographic system such as RSA. This signature is used as the authenticator. As is well known in the art, the signing can be accomplished using a private key created from a public-key pair, where the signing key is only known by the signer, and the other public key is known to the receiving computer. At the payment computer the public key corresponding to each sender is kept in credential database 76. The private key for the payment service is also kept in database 76. At steps 82 or 91, the signature of the received message is checked using the public key known to the receiving computer.

[0061] In a second method for authenticators, at steps 80 or 89, a digest of the payment order is signed by the sending computer with a private key cryptosystem such as DES. This signature is used as the authenticator. At the payment computer, the private key corresponding to each sender is kept in credential database 76. At step 80, a digest of the payment order is signed by the client computer, and at step 89 a digest of the payment order with an added approval code is signed by the payment computer using the same private key. At steps 82 or 91, the signature of the received message is checked using the shared private key.

[0062] In a third method for authenticators, at step 80, the authenticator is computed by a protected device external to the system such as a Smart-Card. A protected device is specifically designed to be extremely difficult both to replicate and to compromise. In this method, the payment order is communicated at 80 to a Smart-Card. The Smart-Card computes and signs a digest of the payment order, and then communicates the signature back at 80 to be used as an authenticator. A Smart-Card produced authenticator uniquely associates a payment order with its creating Smart-Card. This is accomplished by having the Smart-Card contain a secret key "K" that is used to create a digital signature of the payment order. "K" is never released outside of the Smart-card. The Smart-Card is designed to make it computationally infeasible to compute "K" even with possession of the device. In this method, at step 82, a signature checking key from database 76 is used to check the authenticator. In an alternate embodiment, a user must manually signal their acceptance of each payment order on an input device that is part of the external device before the authenticator is created by the external device.

[0063] In a fourth method for authenticators, for use with any of the first to third methods, at steps 80 or 89, a network address is used as an authenticator. At steps 82 or 91, a digest of the payment order is sent back to the specified network address along with a random password. The computer at the specified network address must then return the payment order digest along with the password. If the network guarantees to deliver messages to the proper network address, this method will guarantee that the user or computer at the specified network address approves of the payment order. Assuming that network delivery is trusted, this method can be used to authenticate a sender computer's network address in a payment order. Alternatively, electronic mail can be used to send such confirmation messages between a user and the payment system.

[0064] In a fifth method for authenticators, at step 80 for use with any of the first to third methods, the authenticator is produced by an external device that produces a sequence of non-predictable transaction identifiers that are device specific. The authenticator is entered by the user into the client computer by reading its display. One such device is described in U.S. Patent 4,856,062. According to this method, at step 91, the authenticator can be checked using the sender specific fixed code of the device which is kept in database 76. This sequence of steps is also shown in Figure 15 at steps 93 and 94.

[0065] In a sixth method for authenticators, for use with any of the first to third methods, at step 80, the authenticator is obtained by querying the user for a transaction identifier that is the next string from a physical list of one-time authorization strings. Such as list could be produced on a card, and the user can cross off authorization strings as they are used. According to this meth-

od, at step 91, the authenticator is checked against the next expected string from the sender using database 76. Database 76 can hold for each sender a list of random authorization strings, or can hold a sender specific secret key that was used to generate the list of authentication strings along with how many strings have been used so far. This sequence of steps is also shown in Figure 15 at 93 and 94.

[0066] In a seventh method for authenticators, for use with any of the first to third methods, at step 80 the authenticator is a previously obtained personal identification number (PIN) for the user. In this method in 91 the authenticator is checked against the expected PIN for the sender using database 76.

[0067] As will be obvious to one skilled in the art, any of the methods for creating authenticators can be used together to increase system security. For example, authenticator method six can be used to create an authenticator based on a transaction identifier, and then a payment order including a transaction identifier can be given a further authenticator using authenticator method one. In this example the resulting authenticators would be checked with their respective methods.

[0068] A digest of a payment order can be created with an algorithm such as MD5 [R. Rivest, The MD5 Message-Digest Algorithm, MIT Laboratory for Computer Science, Network Working Group Request for Comments 1321]. Alternatively, a digest can be the entire payment order or other functions of the payment order's component parts.

[0069] In addition in both the sales and payment systems alternate authenticator techniques can be used such as those described by Voydock and Kent in "Security Mechanisms in High-level Network Protocols", Computing Surveys Vol. 15, No. 2, June 1983. As will be appreciated by those skilled in the art, two-way authenticated byte-stream or remote procedure call interface connections that protect against replay can replace our message based authenticators.

Claims

1. A network based payment system (300) comprising:

   a plurality of client computers (70, 71);
   at least one payment computer (72);
   the client computers and the payment computer being interconnected by a public packet switched communications network (69); and
   a financial authorization network (via 78) external to the public packet switched communications network (69), being programmed to authorize payment of a payment amount based on an external credit card account or an external demand deposit account having sufficient credit or funds;
   each one of the client computers (70, 71) being programmed to construct a payment order specifying a payment amount to be transferred from a sender to a beneficiary, a nonce, a sender identifier or account information, and a beneficiary identifier or account information, to sign the payment order with a digital signature of a digest of the payment order, the digital signature authenticating the sender of the payment order, the digital signature being computed based on a secret key, to cause the payment order and the digital signature to be transmitted to the payment computer over the public packet switched communications network (69), and to receive a payment order authorization message from the payment computer;
   the payment computer (72) being programmed to receive the payment order and the digital signature, and in response thereto, to verify that said payment order originated from the sender of the payment order based on the received digital signature, to check for replay to ensure that the sender of the payment order did not previously present a payment order with the same nonce, to cause a message to be transmitted into the financial authorization network, in order to verify that the sender has adequate funds or credit, to receive an authorization from the financial authorization network in response to the message, to transmit a payment order authorization message to the client computer over the public packet switched communications network, to cause information pertaining to the payment order and authorization to be recorded in a settlement database (74), and to cause a financial system network external to the public packet switched communications network (69) to transfer funds from the sender to the beneficiary conditioned on receipt by the payment computer of the authorization from the financial authorization network.

2. A network based payment system in accordance with claim 1, wherein the digest is the entire payment order.

3. A network based payment system in accordance with claim 1, wherein the digest is a function of component parts of the payment order.

4. A network based payment system in accordance with any of claims 1 to 3, wherein the payment order comprises a delivery address, and wherein the payment computer (72) is programmed to cause the delivery address to be checked against a database of allowed delivery addresses for the sender.

5. A network based payment system in accordance

with any preceding claim, wherein the payment computer (72) is programmed to cause at least one allowed delivery address for the sender to be determined, and wherein the payment order authorization message comprises the at least one allowed delivery address.

6. A network based payment system in accordance with any preceding claim, wherein the payment order authorization message comprises an authenticator.

7. A network based payment system in accordance with any preceding claim, wherein the client computer (70, 71) is programmed to generate the digital signature using an external device, and wherein the payment computer (72) is programmed to verify that the digital signature was created using the external device.

8. A method of using a network based payment system (300) comprising a plurality of client computers (70, 71), at least one payment computer (72) interconnected by a public packet switched communications network (69), and a financial authorization network external to the public packet switched communications network (69), comprising the steps of:

constructing a payment order (79) at one of the client computers specifying a payment amount to be transferred from a sender to a beneficiary, a nonce, a sender identifier or account information, and a beneficiary identifier or account information, signing (80) the payment order with a digital signature of a digest of the payment order, the digital signature authenticating the sender of the payment order and being computed based on a secret key, and causing the payment order and the digital signature to be transmitted (81) to the payment computer over the public packet switched communications network (69);
in response to receipt of the payment order and the digital signature by the payment computer verifying (82) that the payment order originates from the sender of the payment order based on the received digital signature, checking for replay (84) to ensure that the sender of the payment order did not previously present a payment order with the same nonce, causing a message to be transmitted (86) into the financial authorization network, in order to verify that the sender has adequate funds or credit;
the financial authorization network authorizing payment of the payment amount based on an external credit card account or an external demand deposit account having sufficient credit or funds;
receiving (87), at the payment computer, an authorization from the financial authorization network in response to the message, transmitting a payment order authorization message (90) from the payment computer to the client computer over the public packet switched communications network, causing information pertaining to the payment order and authorization to be recorded in a settlement database (74), and causing a financial system network external to the public packet switched communications network, to transfer funds from the sender to the beneficiary conditioned on receipt by the payment computer of the authorization from the financial authorization network, and
receiving the payment order authorization message at the client computer.

9. A method in accordance with claim 8, wherein the digest is the entire payment order.

10. A method in accordance with claim 8, wherein the digest is a function of component parts of the payment order.

Patentansprüche

1. Netzwerkgestütztes Zahlungssystem (300) mit:

mehreren Klientencomputern (70, 71),
wenigstens einem Zahlungscomputer (72).

wobei die Klientencomputer und der Zahlungscomputer durch ein öffentliches paketvermitteltes Kommunikationsnetzwerk (69) verbunden sind, und
einem Finanzautorisierungsnetzwerk (via 78) außerhalb des öffentlichen paketvermittelten Kommunikationsnetzwerks (69), das dazu programmiert ist, die Zahlung eines Zahlungsbetrages auf der Grundlage eines externen Kreditkartenkontos oder eines externen Sichteinlagenkontos mit ausreichendem Kredit oder Guthaben zu autorisieren,
wobei jeder der Klientencomputer (70, 71) dazu programmiert ist, eine Zahlungsanweisung zu konstruieren, die einen von einem Absender an einen Zahlungsempfänger zu transferierenden Zahlungsbetrag, ein Augenblickswort, eine Absenderkennung oder -kontoinformation und eine Zahlungsempfängerkennung oder -kontoinformation spezifiziert, die Zahlungsanweisung mit einer digitalen Signatur einer Zusammenfassung der Zahlungsanweisung zu signieren, welche digitale Signatur den Absender der Zahlungsanweisung authentiziert, wobei die digitale Signatur auf der Basis eines geheimen Schlüssels berechnet wird, zu veranlassen, daß die Zahlungsanweisung und die di-

gitale Signatur über das öffentliche paketvermittelte Kommunikationsnetewerk (69) an den Zahlungscomputer übermittelt werden, und eine Zahlungsanweisungs-Autorisierungsnachricht vom Zahlungscomputer zu empfangen,

wobei der Zahlungscomputer (72) dazu programmlert ist, die Zahlungsanweisung und die digitale Signatur zu empfangen und als Reaktion darauf anhand der empfangenen digitalen Signatur zu verifizieren, daß die Zahlungsanweisung vom Absender der Zahlungsanweisung stammt, eine Überprüfung auf Wiedergabe einer Aufzeichnung durchzuführen, um sicherzustellen, daß der Absender der Zahlungsanweisung nicht früher eine Zahlungsanweisung mit demselben Augenblickswort präsentiert hat, zu veranlassen, daß eine Nachricht in das Finanzautorisierungsnetzwerk übermittelt wird. um zu verifizieren, daß der Absender ein adäquates Guthaben oder Kredit hat, als Antwort auf die Nachricht eine Autorisierung vom Finanzautorisierungsnetzwerk zu empfangen, eine Zahlungsanweisungs-Autorisierungsnachricht über das öffentliche paketvermittelte Kommunikationsnetzwerk an den Klientencomputer zu übermitteln, zu veranlassen, daß Information über die Zahlungsanweisung und die Autorisierung in einer Abwicklungsdatenbank (74) aufgezeichnet wird, und, konditioniert dadurch, daß der Zahlungscomputer die Autorisierung vom Finanzautorisierungsnetzwerk empfängt, ein Finanzsystem-Netzwerk außerhalb des öffentlichen paketvermittelten Kommunikationsnetzwerkes (69) zu veranlassen, Guthaben vom Absender an den Zahlungsempfänger zu transferieren.

2. Netzwerkgestütztes Zahlungssystem nach Anspruch 1, bei dem die Zusammenfassung die gesamte Zahlungsanweisung ist.

3. Netzwerkgestütztes Zahlungssystem nach Anspruch 1, bei dem die Zusammenfassung eine Punktion von Bestandteilen der Zahlungsanweisung ist.

4. Netzwerkgestütztes Zahlungssystem nach einem der Ansprüche 1 bis 3, bei dem die Zahlungsanweisung eine Zustelladresse enthält und der Zahlungscomputer (72) dazu programmiert ist, zu veranlassen, daß die Zustelladresse gegen eine Datenbank von zulässigen Zustelladressen für den Absender geprüft wird.

5. Netzwerkgestütztes Zahlungssystem nach irgendeinern vorstehenden Anspruch, bei dem der Zahlungscomputer (72) dazu programmiert ist, zu veranlassen, daß wenigstens eine zulässige Zustelladresse für den Absender bestimmt wird, und die Zahlungsanwelsungs-Autorisierungsnachricht die wenigstens eine zulässige Zustelladresse enthält.

6. Netzwerkgestütztes Zahlungssystem nach irgendeinem vorstehenden Anspruch, bei dem die Zahlungsanwelsungs-Autorisierungsnachricht eine Authentifizierung enthält.

7. Netzwerkgestütztes Zahlungssystem nach irgendeinem vorstehenden Anspruch, bei dem der Klientencomputer (70, 71) dazu programmiert ist, die digitale Signatur mit Hilfe einer externen Einrichtung zu erzeugen, und der Zahlungscomputer (72) dazu programmiert ist, zu verifizieren, daß die digitale Signatur mit Hilfe der externen Einrichtung erzeugt wurde.

8. Verfahren zum Gebrauch eines netzwerkgestützten Zahlungssystems (300) mit mehreren Klientencomputern (70, 71), wenigstens einem durch ein öffentliches paketvermitteltes Kommunikationsnetzwerk (69) verbundenen Zahlungscomputer (72) und einem Finanzautorisierungsnetzwerk außerhalb des öffentlichen paketvermittelten Kommunikationsnetzwerkes (69), mit den Schritten:

Konstruieren einer Zahlungsanweisung (79) an einem der Klientencomputer, die einen von einem Absender an einen Zahlungsempfänger zu transferierenden Zahlungsbetrag, ein Augenblickswort, eine Absenderkennung oder -kontoinformation und eine Zahlungsempfängerkennung oder -kontoinformation spezifiziert, Signieren (80) der Zahlungsanweisung mit einer digitalen Signatur einer Zusammenfassung der Zahlungsanweisung, wobei die digitale Signatur den Absender der Zahlungsanweisung authentiziert und auf der Grundlage eines geheimen Schlüssels berechnet wird, und Veranlassen, daß die Zahlungsanweisung und die digitale Signatur über das öffentliche paketvermittelte Kommunikationsnetzwerk (69) an den Zahlungscomputer übermittelt (81) werden,
als Reaktion auf den Empfang der Zahlungsanweisung und der digitalen Signatur durch den Zahlungscomputer, verifizieren (82), daß die Zahlungsanweisung vom Absender der Zahlungsanweisung stammt, anhand der empfangenen digitalen Signatur, Prüfen auf Wiedergabe (84) einer Aufzeichnung, um sicherzustellen, daß der Absender der Zahlungsanweisung nicht früher eine Zahlungsanweisung mit demselben Augenblickswort präsentiert hat, veranlassen, daß eine Nachricht in das Finanzautorisierungsnetzwerk übermittelt (86) wird, um zu verifizieren, daß der Absender ein adäquates Guthaben oder Kredit hat,

wobei das Finanzauthorisierungsnetzwerk die Zahlung des Zahlungsbetrages auf der Grund-

lage eines externen Kreditkartenkontos oder eines externen Sichteinlagenkontos mit ausreichendem Kredit oder Guthaben autorisiert,

Empfangen (87), am Zahlungscomputer, einer Autorisierung vom Finanzauthorisierungsnetzwerk als Reaktion auf die Nachricht. Übermitteln einer Zahlungsanweisungs-Autorisierungsnachricht (90) vom Zahlungscomputer an den Klientencomputer über das öffentliche paketvermittelte Kommunikationsnetzwerk. Veranlassen, daß Information über die Zahlungsanweisung und Autorisierung in einer Abwicklungsdatenbank (74) aufgezeichnet werden, und Veranlassen eines Finanzsystem-Netzwerks außerhalb des öffentlichen paketvermittelten Kommunikationsnetzwerkes, Guthaben vom Absender an den Zahlungsempfänger zu transferieren, konditioniert dadurch, daß der Zahlungscomputer die Autorisierung vom Finanzautorisierungsnetzwerk empfängt, und

Empfangen der Zahlungsanweisungs-Autorisierungsnachricht am Klienten-Computer.

9. Verfahren nach Anspruch 8, bei dem die Zusammenfassung die gesamte Zahlungsanweisung ist.

10. Verfahren nach Anspruch 8, bei dem die Zusammenfassung eine Funktion von Bestandteilen der Zahlungsanweisung ist.

Revendications

1. Système de paiement basé sur un réseau informatique (300), comprenant :

une pluralité d'ordinateurs clients (70,71),

au moins un ordinateur de paiement (72),

les ordinateurs clients et l'ordinateur de paiement étant reliés entre eux par un réseau public de communications commuté par paquets (69) ; et

un réseau d'autorisation financière (via 78) extérieur au réseau public de communications commuté par paquets (69) étant programmé pour autoriser le paiement d'un montant de paiement sur la base d'un compte extérieur de carte de crédit ou d'un compte extérieur de dépôt à vue disposant d'un crédit suffisant ou de fonds suffisants ;

chacun des ordinateurs clients (70,71), étant programmé pour établir un ordre de paiement spécifiant un montant de paiement à transférer d'un expéditeur à un bénéficiaire, un mot créé, un identificateur ou une information de compte concernant l'expéditeur, et un identificateur ou une information de compte concernant le bénéficiaire, pour signer l'ordre de paiement avec une signature numérique d'un abrégé de l'ordre de paiement, la signature numérique authentifiant l'expéditeur de l'ordre de paiement, la signature numérique étant informatisée sur la base d'une clé secrète, pour permettre la transmission de l'ordre de paiement et de la signature numérique à l'ordinateur de paiement sur le réseau public de communications commuté par paquets (69), et pour recevoir un message d'autorisation d'ordre de paiement de la part de l'ordinateur de paiement ;

l'ordinateur de paiement (72) étant programmé pour recevoir l'ordre de paiement et la signature numérique, et en réponse à cela, pour vérifier que le dit ordre de paiement provient bien de l'expéditeur de l'ordre de paiement sur la base de la signature numérique reçue, pour vérifier une répétition afin de s'assurer que l'expéditeur de l'ordre de paiement n'a pas présenté antérieurement un ordre de paiement ayant le même mot créé, pour provoquer la transmission d'un message dans le réseau d'autorisation financière, afin de vérifier que l'expéditeur dispose de fonds ou d'un crédit appropriés, pour recevoir une autorisation de la part du réseau d'autorisation financière en réponse au message, pour transmettre un message d'autorisation d'ordre de paiement à l'ordinateur client sur le réseau public de communications commuté par paquets, pour faire que l'information appartenant à l'ordre de paiement et à l'autorisation soit enregistrée dans une base de données de règlement (74), et pour faire transférer par un réseau public de communications commuté par paquets (69) des fonds de l'expéditeur au bénéficiaire sous la condition de la réception par l'ordinateur de paiement de l'autorisation provenant du réseau d'autorisation financière.

2. Système de paiement basé sur un réseau informatique selon la revendication 1, dans lequel l'abrégé est constitué par l'ordre de paiement entier.

3. Système de paiement basé sur un réseau informatique selon la revendication 1, dans lequel l'abrégé est une fonction des parties constitutives de l'ordre de paiement.

4. Système de paiement basé sur un réseau informatique selon l'une quelconque des revendications 1 à 3, dans lequel l'ordre de paiement comprend une adresse de livraison, et dans lequel l'ordinateur de paiement (72) est programmé pour faire vérifier

l'adresse de livraison dans une base de données d'adresses de livraison autorisées de l'expéditeur.

5. Système de paiement basé sur un réseau informatique selon l'une quelconque des revendications précédentes, dans lequel l'ordinateur de paiement (72) est programmé pour déterminer au moins une adresse de livraison autorisée de l'expéditeur, et dans lequel le message d'autorisation d'ordre de paiement comprend la au moins une adresse de livraison autorisée.

6. Système de paiement basé sur un réseau informatique selon l'une quelconque des revendications précédentes, dans lequel le message d'autorisation d'ordre de paiement comprend un authentificateur.

7. Système de paiement basé sur un réseau informatique selon l'une quelconque des revendications précédentes, dans lequel l'ordinateur client (70,71) est programmé pour produire la signature numérique en utilisant un dispositif extérieur, et dans lequel l'ordinateur de paiement (72) est programmé pour vérifier que la signature numérique a été créée en utilisant le dispositif extérieur.

8. Procédé d'utilisation d'un système de paiement basé sur un réseau informatique (300) comprenant une pluralité d'ordinateurs clients (70, 71), au moins un ordinateur de paiement (72) reliés ensemble par un réseau public de communications commuté par paquets (69), et un réseau d'autorisation financière extérieur au réseau public de communications commuté par paquets, comprenant les opérations consistant :

à établir à l'un des ordinateurs clients un ordre de paiement (79) spécifiant un montant de paiement à transférer d'un expéditeur à un bénéficiaire, un mot créé, un identificateur ou une information de compte de l'expéditeur, et un identificateur ou une information de compte du bénéficiaire, à signer (80) l'ordre de paiement par une signature numérique d'un abrégé de l'ordre de paiement, la signature numérique authentifiant l'expéditeur de l'ordre de paiement et étant informatisée sur la base d'une clé secrète, et à faire transmettre (81) l'ordre de paiement et la signature numérique à l'ordinateur de paiement sur le réseau public de communications commuté par paquets (69),

en réponse à la réception de l'ordre de paiement et de la signature numérique par l'ordinateur de paiement, à vérifier (82) que l'ordre de paiement provient de l'expéditeur de l'ordre de paiement sur la base de la signature numérique reçue, à vérifier une répétition (84) pour s'assurer que l'expéditeur de l'ordre de paiement n'avait pas présenté antérieurement un ordre de paiement avec le même mot créé, à faire transmettre (86) un message dans le réseau d'autorisation financière, afin de vérifier que l'expéditeur dispose de fonds ou d'un crédit appropriés,

le réseau d'autorisation financière autorise le paiement du montant de paiement sur la base d'une compte extérieur de carte de crédit ou d'un compte extérieur de dépôt à vue disposant d'un crédit ou de fonds suffisants ;

à recevoir (87), à l'ordinateur de paiement, une autorisation de la part du réseau d'autorisation financière en réponse au message, à transmettre un message d'autorisation d'ordre de paiement (90) depuis l'ordinateur de paiement à l'ordinateur client sur le réseau public de communications commuté par paquets, à faire enregistrer dans une base de données de règlement (74) l'information appartenant à l'ordre de paiement et à l'autorisation, et à faire transférer, par un réseau de système financier extérieur, au réseau public de communications commuté par paquets, des fonds depuis l'expéditeur vers le bénéficiaire sous la condition de la réception par l'ordinateur de paiement de l'autorisation provenant du réseau d'autorisation financière, et

à recevoir à l'ordinateur client le message d'autorisation d'ordre de paiement.

9. Procédé selon la revendication 8, selon lequel l'abrégé est constitué par l'ordre de paiement entier.

10. Procédé selon la revendication 8, selon lequel l'abrégé est fonction des parties constitutives de l'ordre de paiement.

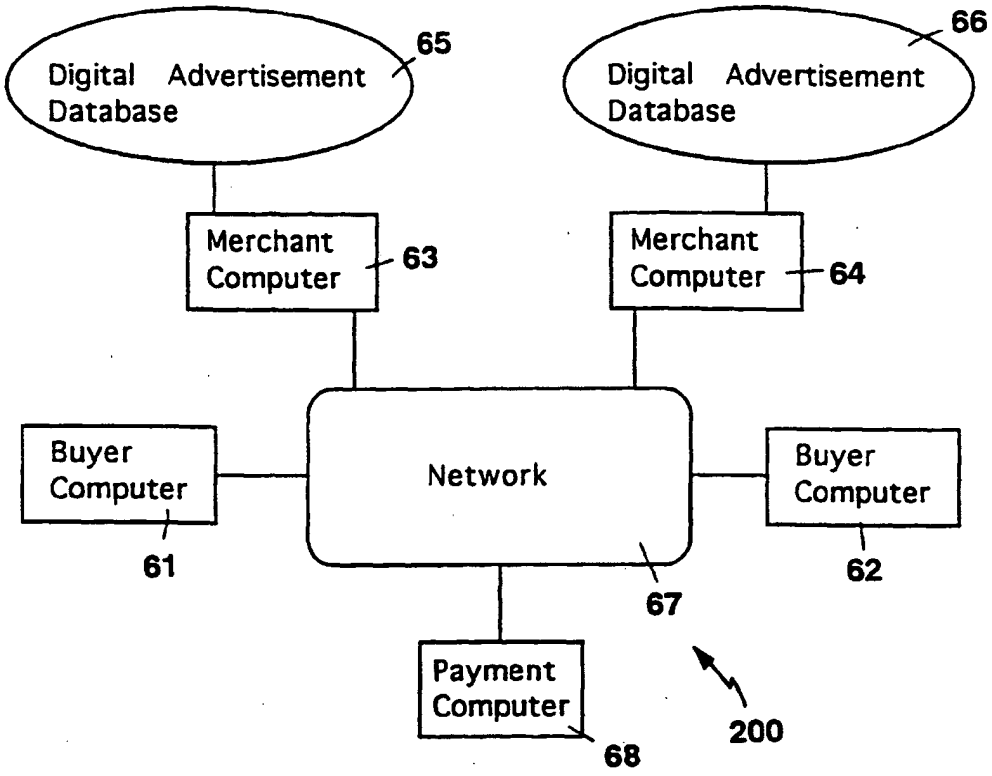
Digital Advertisement Database
65
Digital Advertisement Database
66
Merchant Computer
63
Merchant Computer
64
Buyer Computer
61
Network
Buyer Computer
62
67
Payment Computer
68
200

FIG. 1

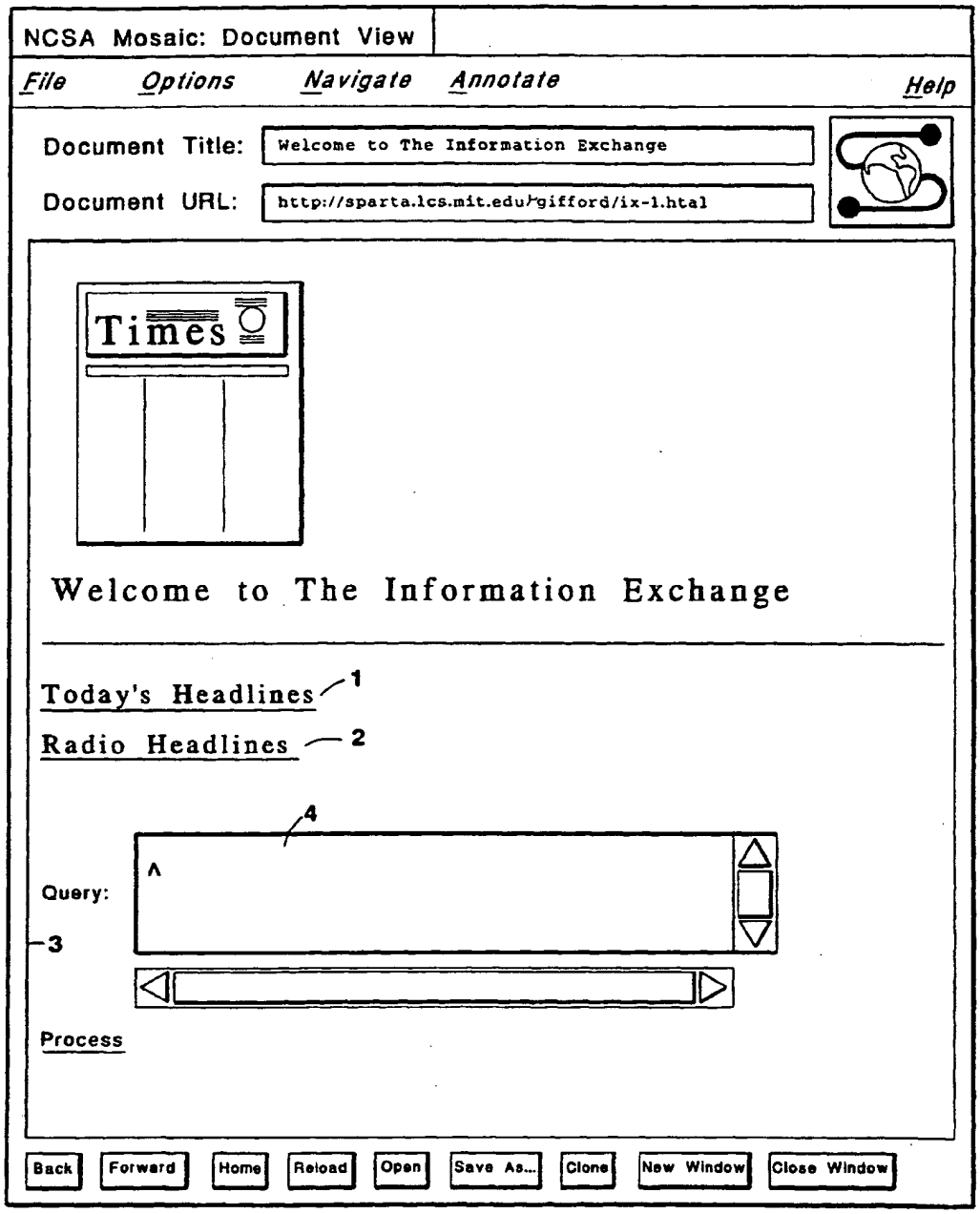
NCSA Mosaic: Document View
File
Options
Navigate
Annotate
Help
Document Title:
Welcome to The Information Exchange
Document URL:
http://sparta.lcs.mit.edu/gifford/ix-1.html
Times
Welcome to The Information Exchange
Today's Headlines
1
Radio Headlines
2
4
Query:
3
Process
Back
Forward
Home
Reload
Open
Save As...
Clone
New Window
Close Window

FIG. 2

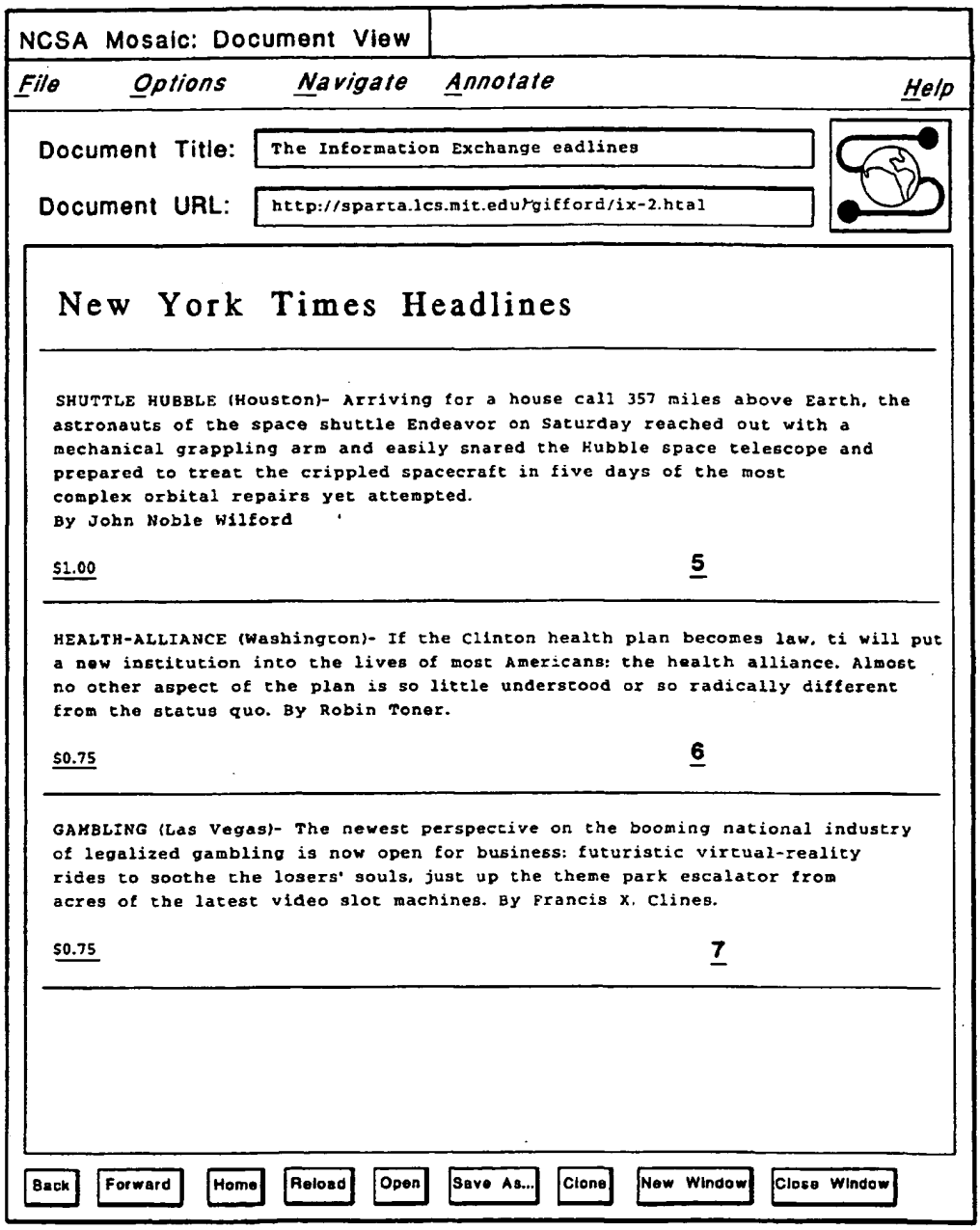
NCSA Mosaic: Document View
File
Options
Navigate
Annotate
Help
Document Title:
The Information Exchange eadlines
Document URL:
http://sparta.lcs.mit.edu/gifford/ix-2.html
New York Times Headlines
SHUTTLE HUBBLE (Houston)- Arriving for a house call 357 miles above Earth, the astronauts of the space shuttle Endeavor on Saturday reached out with a mechanical grappling arm and easily snared the Hubble space telescope and prepared to treat the crippled spacecraft in five days of the most complex orbital repairs yet attempted.
By John Noble Wilford
$1.00
5
HEALTH-ALLIANCE (Washington)- If the Clinton health plan becomes law, ti will put a new institution into the lives of most Americans: the health alliance. Almost no other aspect of the plan is so little understood or so radically different from the status quo. By Robin Toner.
$0.75
6
GAMBLING (Las Vegas)- The newest perspective on the booming national industry of legalized gambling is now open for business: futuristic virtual-reality rides to soothe the losers' souls, just up the theme park escalator from acres of the latest video slot machines. By Francis X. Clines.
$0.75
7
Back
Forward
Home
Reload
Open
Save As...
Clone
New Window
Close Window

FIG. 3

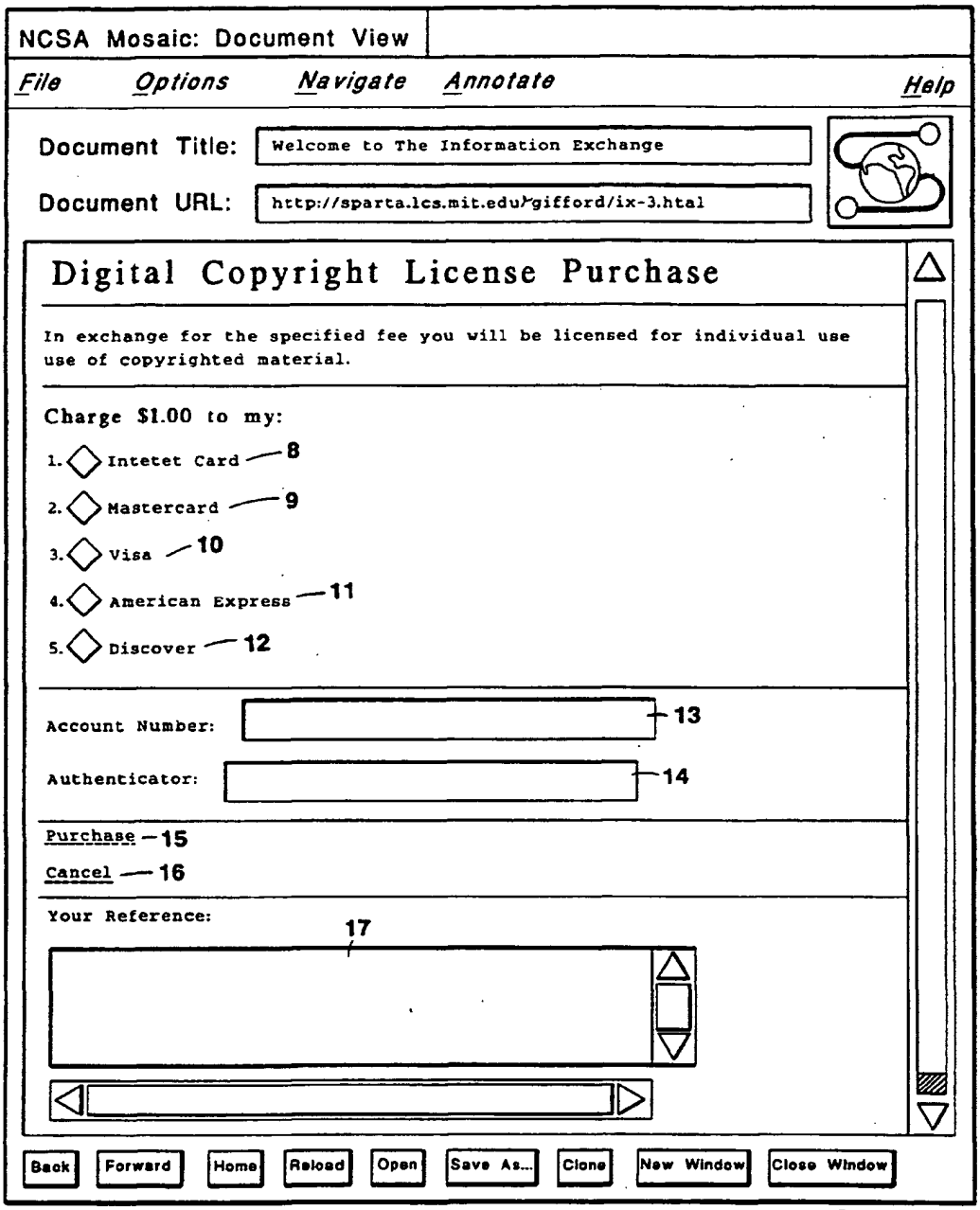
NCSA Mosaic: Document View
File
Options
Navigate
Annotate
Help
Document Title:
Welcome to The Information Exchange
Document URL:
http://sparta.lcs.mit.edu:gifford/ix-3.html
Digital Copyright License Purchase
In exchange for the specified fee you will be licensed for individual use use of copyrighted material.
Charge $1.00 to my:
1. Intetet Card
2. Mastercard
3. Visa
4. American Express
5. Discover
8
9
10
11
12
Account Number:
Authenticator:
13
14
Purchase
Cancel
15
16
Your Reference:
17
Back
Forward
Home
Reload
Open
Save As...
Clone
New Window
Close Window

FIG. 4

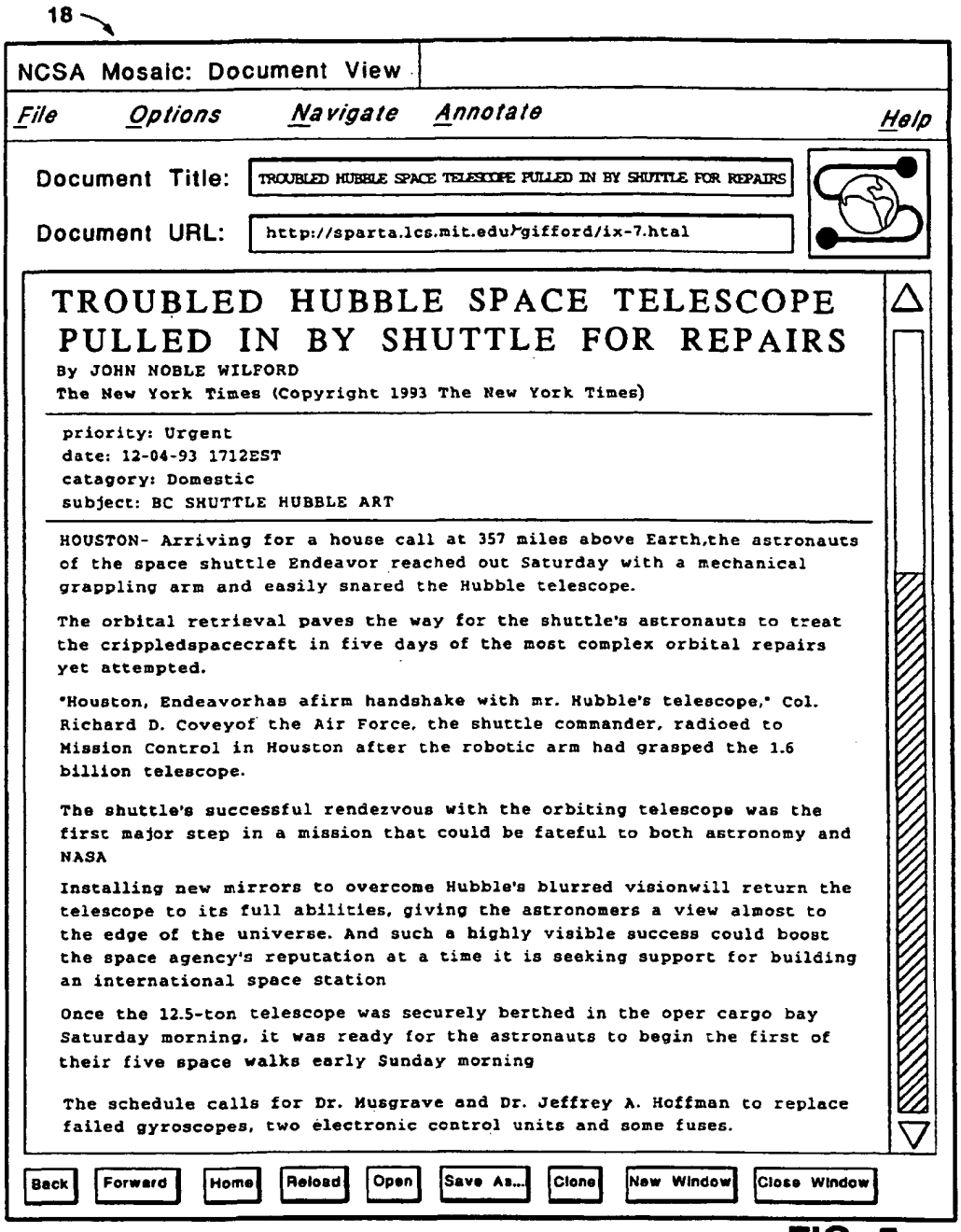
18
NCSA Mosaic: Document View
File
Options
Navigate
Annotate
Help
Document Title:
TROUBLED HUBBLE SPACE TELESCOPE PULLED IN BY SHUTTLE FOR REPAIRS
Document URL:
http://sparta.lcs.mit.edu/gifford/ix-7.htal
TROUBLED HUBBLE SPACE TELESCOPE PULLED IN BY SHUTTLE FOR REPAIRS
By JOHN NOBLE WILFORD
The New York Times (Copyright 1993 The New York Times)
priority: Urgent
date: 12-04-93 1712EST
catagory: Domestic
subject: BC SHUTTLE HUBBLE ART
HOUSTON- Arriving for a house call at 357 miles above Earth,the astronauts of the space shuttle Endeavor reached out Saturday with a mechanical grappling arm and easily snared the Hubble telescope.
The orbital retrieval paves the way for the shuttle's astronauts to treat the crippledspacecraft in five days of the most complex orbital repairs yet attempted.
"Houston, Endeavorhas afirm handshake with mr. Hubble's telescope," Col. Richard D. Coveyof the Air Force, the shuttle commander, radioed to Mission Control in Houston after the robotic arm had grasped the 1.6 billion telescope.
The shuttle's successful rendezvous with the orbiting telescope was the first major step in a mission that could be fateful to both astronomy and NASA
Installing new mirrors to overcome Hubble's blurred visionwill return the telescope to its full abilities, giving the astronomers a view almost to the edge of the universe. And such a highly visible success could boost the space agency's reputation at a time it is seeking support for building an international space station
Once the 12.5-ton telescope was securely berthed in the oper cargo bay Saturday morning, it was ready for the astronauts to begin the first of their five space walks early Sunday morning
The schedule calls for Dr. Musgrave and Dr. Jeffrey A. Hoffman to replace failed gyroscopes, two electronic control units and some fuses.
Back
Forward
Home
Reload
Open
Save As...
Clone
New Window
Close Window

FIG. 5

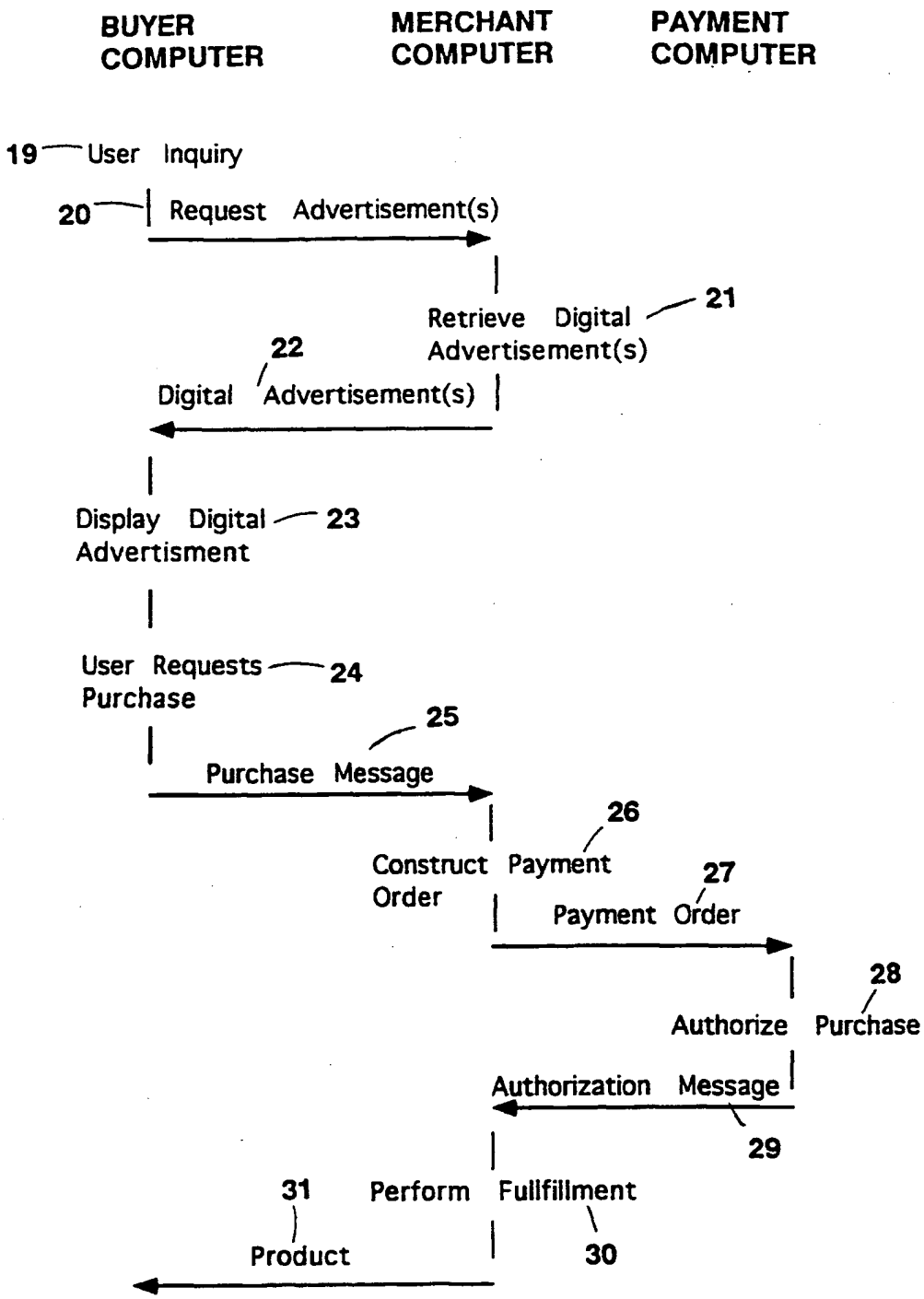
BUYER COMPUTER
MERCHANT COMPUTER
PAYMENT COMPUTER
19
User Inquiry
20
Request Advertisement(s)
Retrieve Digital Advertisement(s)
21
22
Digital Advertisement(s)
Display Digital Advertisment
23
User Requests Purchase
24
25
Purchase Message
26
Construct Order
Payment Order
27
Payment Order
28
Authorize Purchase
Authorization Message
29
31
Perform Fullfillment
Product
30

FIG. 6

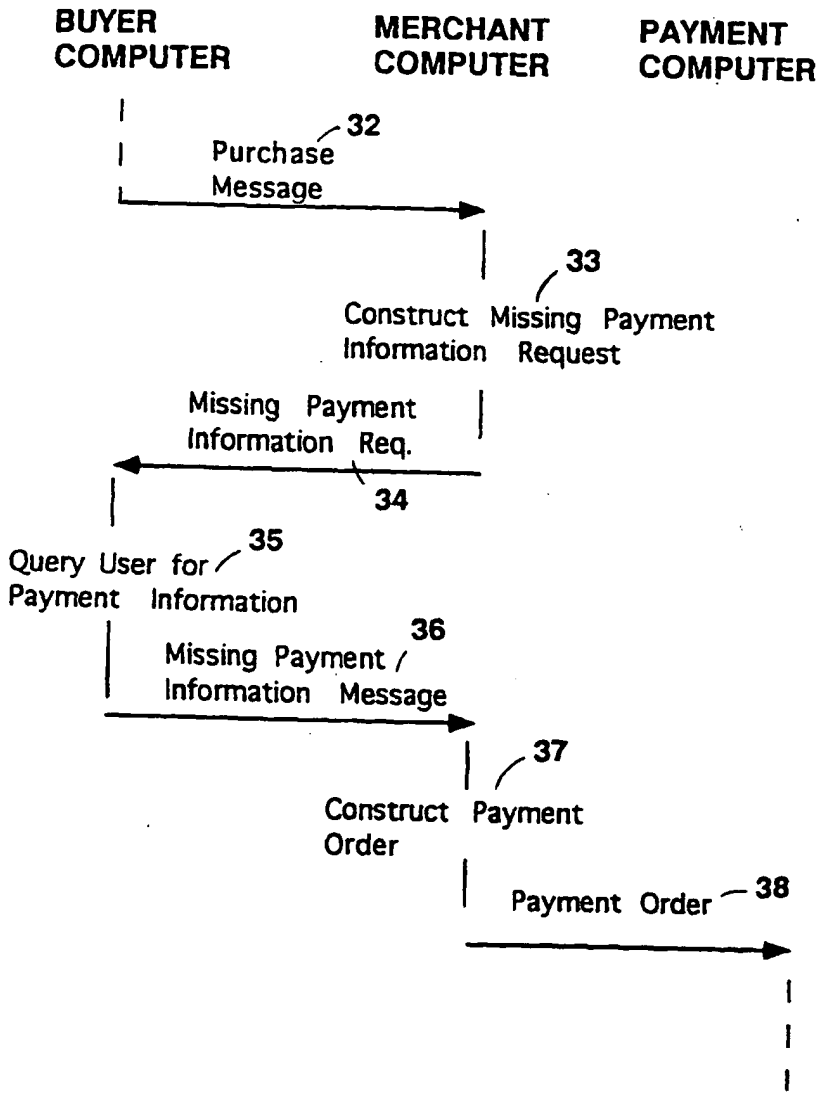
BUYER COMPUTER
MERCHANT COMPUTER
PAYMENT COMPUTER
32
Purchase Message
33
Construct Missing Payment Information Request
Missing Payment Information Req.
34
35
Query User for Payment Information
36
Missing Payment Information Message
37
Construct Payment Order
Payment Order
38

FIG. 7

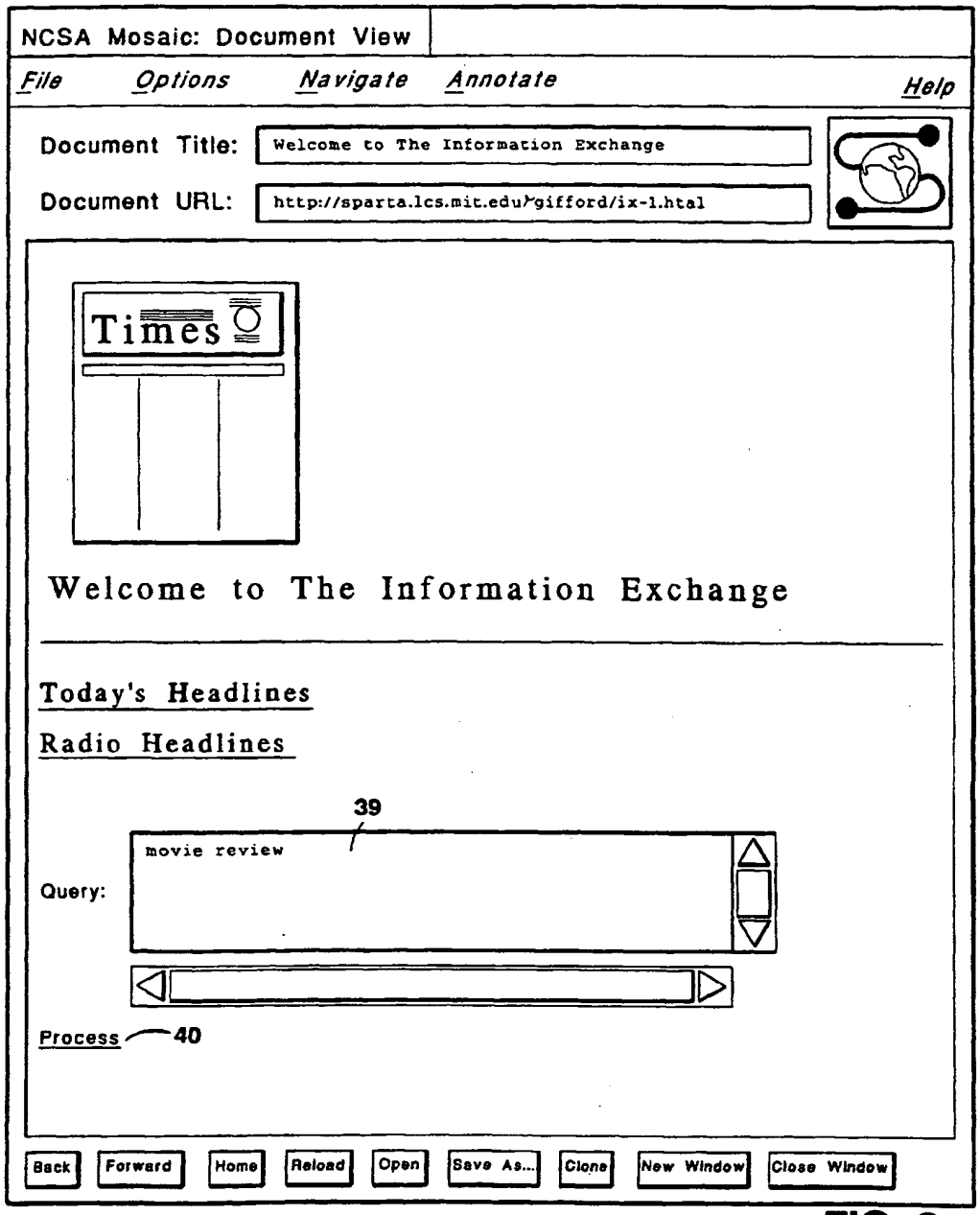
NCSA Mosaic: Document View
File
Options
Navigate
Annotate
Help
Document Title:
Welcome to The Information Exchange
Document URL:
http://sparta.lcs.mit.edu/gifford/ix-1.html
Times
Welcome to The Information Exchange
Today's Headlines
Radio Headlines
39
movie review
Query:
Process
40
Back
Forward
Home
Reload
Open
Save As...
Clone
New Window
Close Window

FIG. 8

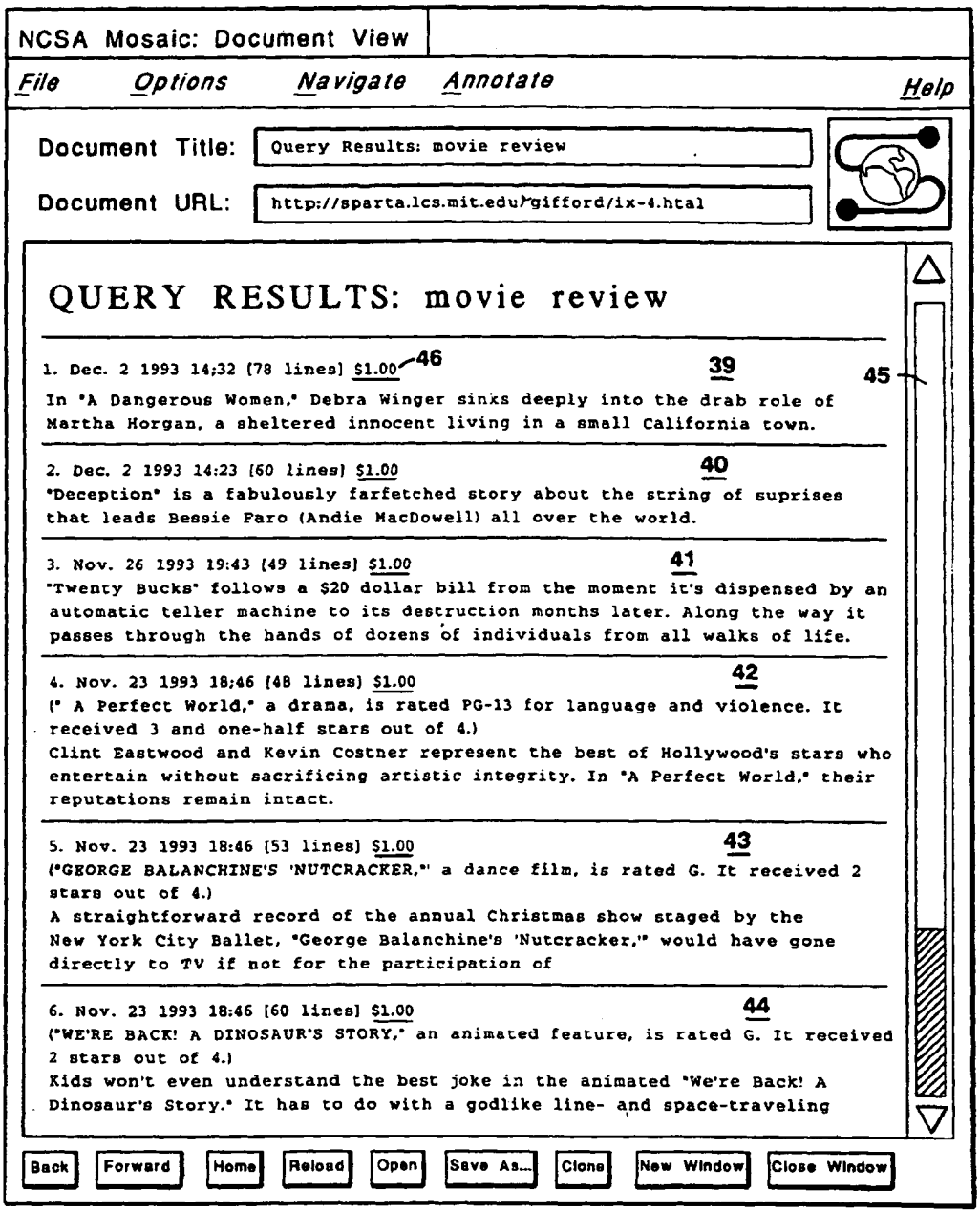
NCSA Mosaic: Document View
File
Options
Navigate
Annotate
Help
Document Title:
Query Results: movie review
Document URL:
http://sparta.lcs.mit.edu/gifford/ix-4.html
QUERY RESULTS: movie review
1. Dec. 2 1993 14:32 (78 lines) $1.00
46
39
45
In "A Dangerous Women," Debra Winger sinks deeply into the drab role of Martha Horgan, a sheltered innocent living in a small California town.
2. Dec. 2 1993 14:23 (60 lines) $1.00
40
"Deception" is a fabulously farfetched story about the string of suprises that leads Bessie Faro (Andie MacDowell) all over the world.
3. Nov. 26 1993 19:43 (49 lines) $1.00
41
"Twenty Bucks" follows a $20 dollar bill from the moment it's dispensed by an automatic teller machine to its destruction months later. Along the way it passes through the hands of dozens of individuals from all walks of life.
4. Nov. 23 1993 18:46 (48 lines) $1.00
42
(" A Perfect World," a drama, is rated PG-13 for language and violence. It received 3 and one-half stars out of 4.)
Clint Eastwood and Kevin Costner represent the best of Hollywood's stars who entertain without sacrificing artistic integrity. In "A Perfect World," their reputations remain intact.
5. Nov. 23 1993 18:46 (53 lines) $1.00
43
("GEORGE BALANCHINE'S 'NUTCRACKER,'" a dance film, is rated G. It received 2 stars out of 4.)
A straightforward record of the annual Christmas show staged by the New York City Ballet, "George Balanchine's 'Nutcracker,'" would have gone directly to TV if not for the participation of
6. Nov. 23 1993 18:46 (60 lines) $1.00
44
("WE'RE BACK! A DINOSAUR'S STORY," an animated feature, is rated G. It received 2 stars out of 4.)
Kids won't even understand the best joke in the animated "We're Back! A Dinosaur's Story." It has to do with a godlike line- and space-traveling
Back
Forward
Home
Reload
Open
Save As...
Clone
New Window
Close Window

FIG. 9

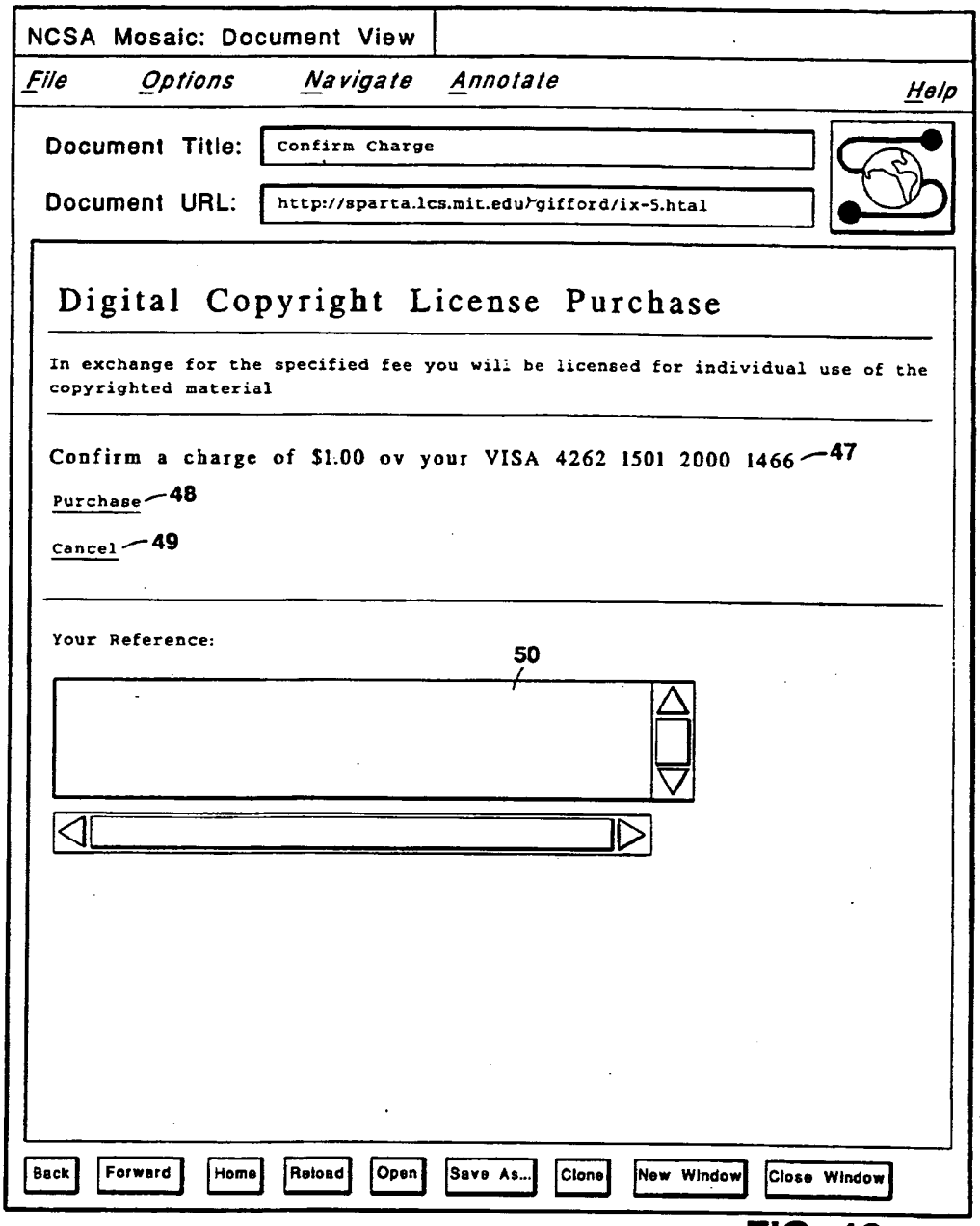
NCSA Mosaic: Document View
File
Options
Navigate
Annotate
Help
Document Title:
Confirm Charge
Document URL:
http://sparta.lcs.mit.edu/gifford/ix-5.html
Digital Copyright License Purchase
In exchange for the specified fee you will be licensed for individual use of the copyrighted material
Confirm a charge of $1.00 ov your VISA 4262 1501 2000 1466
47
Purchase
48
Cancel
49
Your Reference:
50
Back
Forward
Home
Reload
Open
Save As...
Clone
New Window
Close Window

FIG. 10

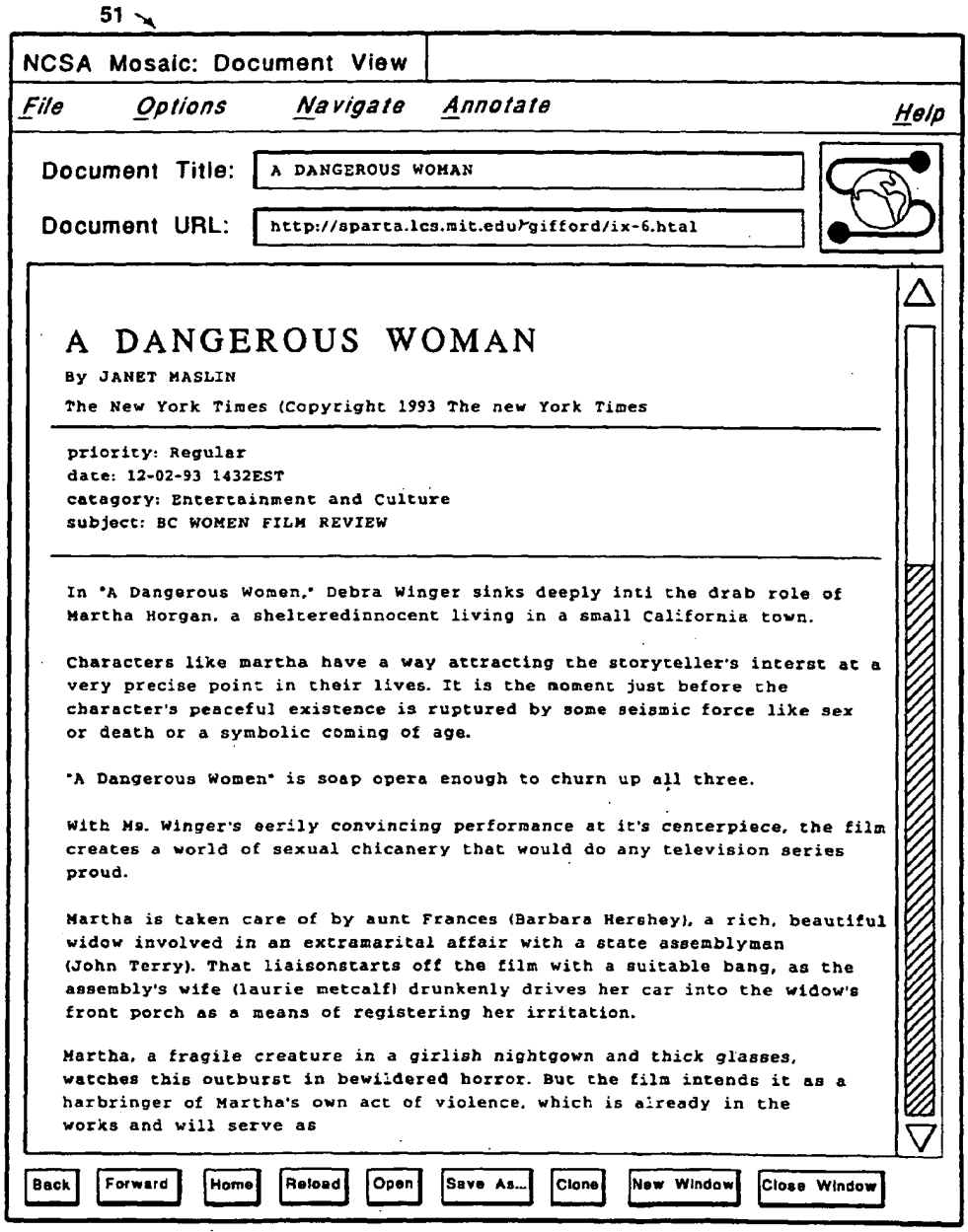
51
NCSA Mosaic: Document View
File
Options
Navigate
Annotate
Help
Document Title:
A DANGEROUS WOMAN
Document URL:
http://sparta.lcs.mit.edu/gifford/ix-6.htal
A DANGEROUS WOMAN
By JANET MASLIN
The New York Times (Copyright 1993 The new York Times
priority: Regular
date: 12-02-93 1432EST
catagory: Entertainment and Culture
subject: BC WOMEN FILM REVIEW
In "A Dangerous Women," Debra Winger sinks deeply inti the drab role of Martha Horgan, a shelteredinnocent living in a small California town.
Characters like martha have a way attracting the storyteller's interst at a very precise point in their lives. It is the moment just before the character's peaceful existence is ruptured by some seismic force like sex or death or a symbolic coming of age.
"A Dangerous Women" is soap opera enough to churn up all three.
With Ms. Winger's eerily convincing performance at it's centerpiece, the film creates a world of sexual chicanery that would do any television series proud.
Martha is taken care of by aunt Frances (Barbara Hershey), a rich, beautiful widow involved in an extramarital affair with a state assemblyman (John Terry). That liaisonstarts off the film with a suitable bang, as the assembly's wife (laurie metcalf) drunkenly drives her car into the widow's front porch as a means of registering her irritation.
Martha, a fragile creature in a girlish nightgown and thick glasses, watches this outburst in bewildered horror. But the film intends it as a harbringer of Martha's own act of violence, which is already in the works and will serve as
Back
Forward
Home
Reload
Open
Save As...
Clone
New Window
Close Window

FIG. 11

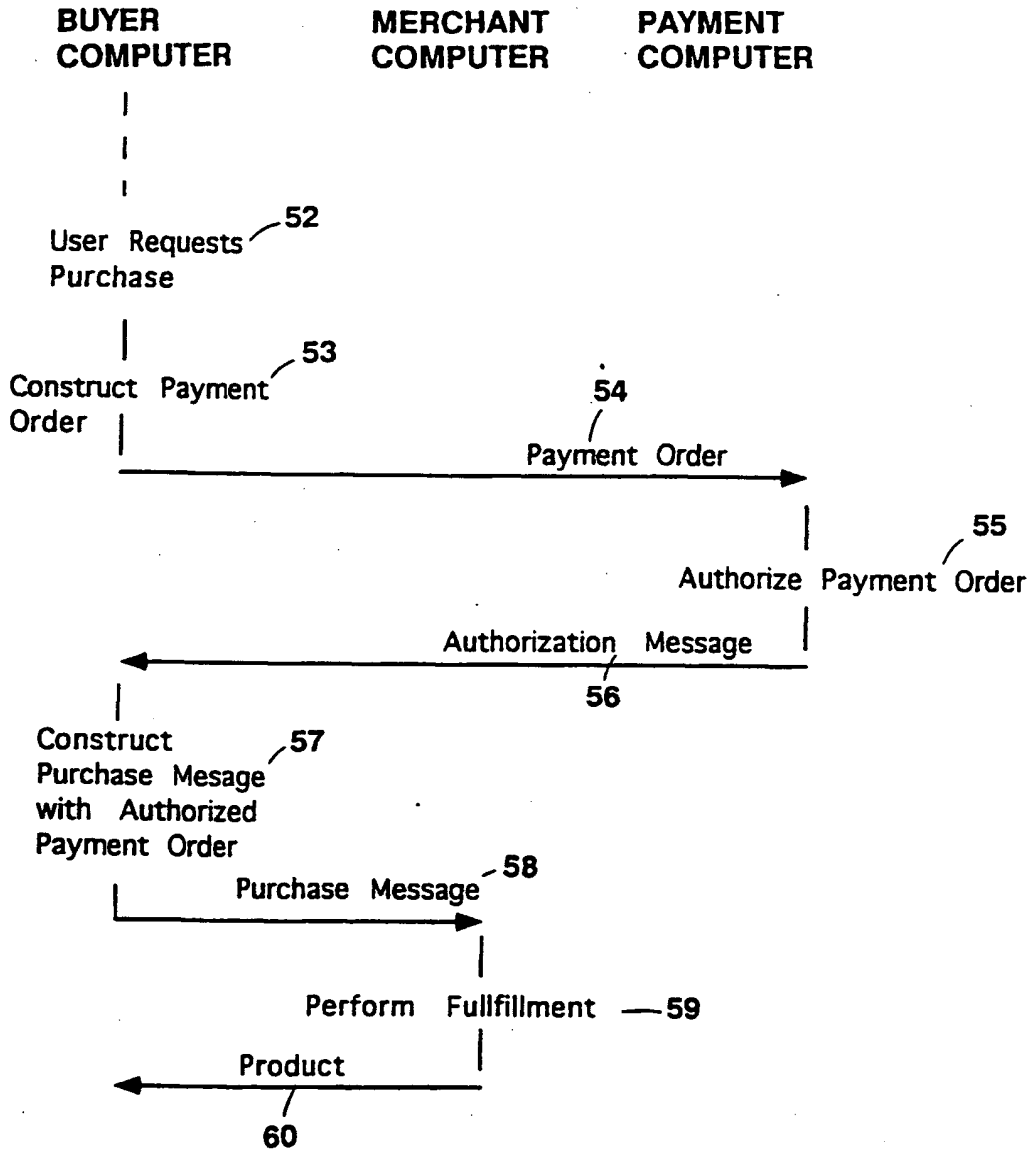
BUYER COMPUTER
MERCHANT COMPUTER
PAYMENT COMPUTER
User Requests Purchase
52
Construct Payment Order
53
54
Payment Order
55
Authorize Payment Order
Authorization Message
56
Construct Purchase Mesage with Authorized Payment Order
57
Purchase Message
58
Perform Fullfillment
59
Product
60

FIG. 12

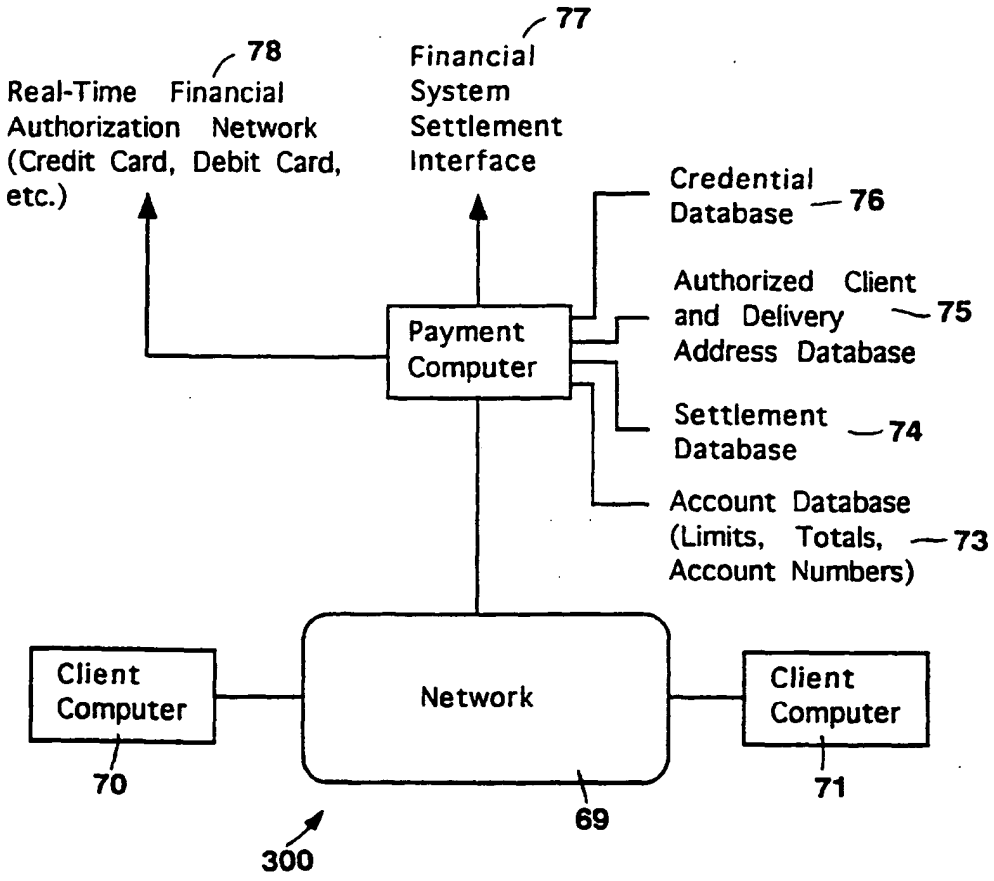
78
Real-Time Financial Authorization Network (Credit Card, Debit Card, etc.)
77
Financial System Settlement Interface
Credential Database 76
Authorized Client and Delivery Address Database 75
Payment Computer
Settlement Database 74
Account Database (Limits, Totals, Account Numbers) 73
Client Computer
70
Network
69
Client Computer
71
300

FIG. 13

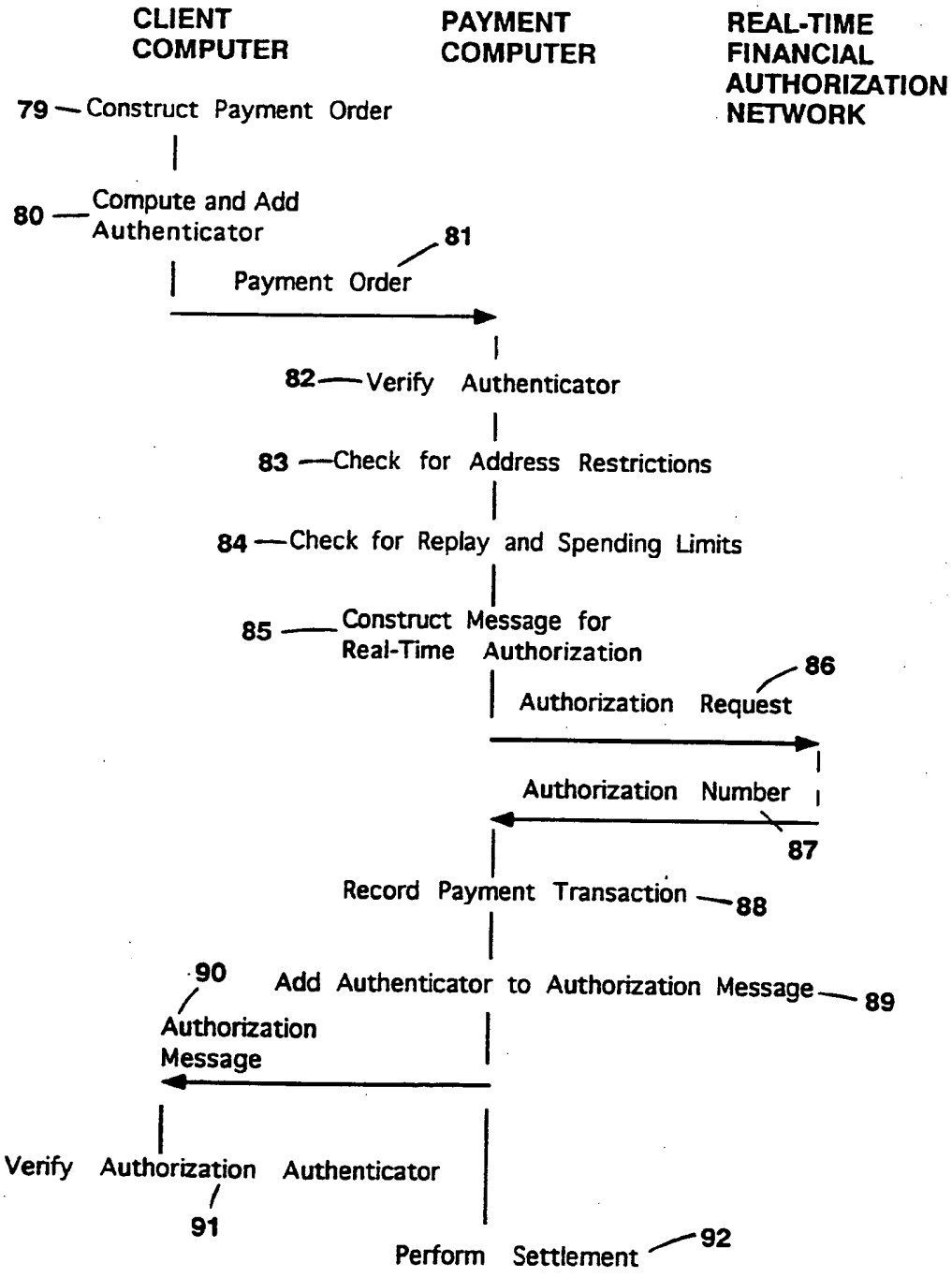
CLIENT COMPUTER
PAYMENT COMPUTER
REAL-TIME FINANCIAL AUTHORIZATION NETWORK
79 Construct Payment Order
80 Compute and Add Authenticator
81
Payment Order
82 Verify Authenticator
83 Check for Address Restrictions
84 Check for Replay and Spending Limits
85 Construct Message for Real-Time Authorization
86
Authorization Request
Authorization Number
87
Record Payment Transaction 88
90
Add Authenticator to Authorization Message 89
Authorization Message
Verify Authorization Authenticator
91
Perform Settlement 92

FIG. 14

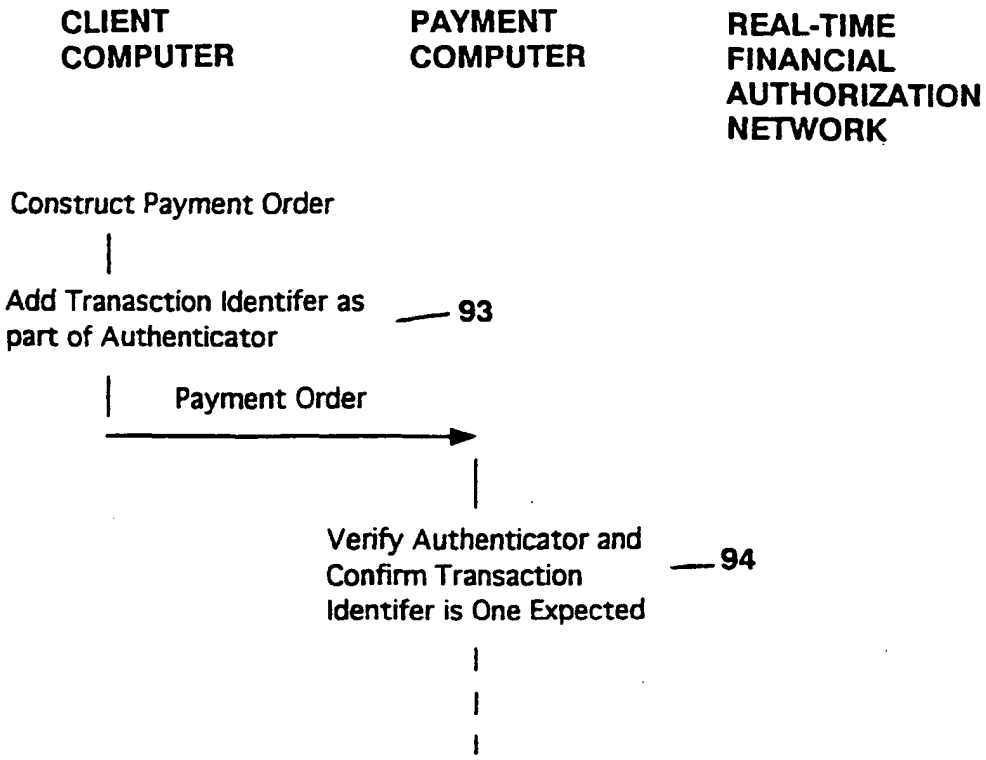
CLIENT COMPUTER
PAYMENT COMPUTER
REAL-TIME FINANCIAL AUTHORIZATION NETWORK
Construct Payment Order
Add Tranasction Identifer as part of Authenticator
93
Payment Order
Verify Authenticator and Confirm Transaction Identifer is One Expected
94

FIG. 15

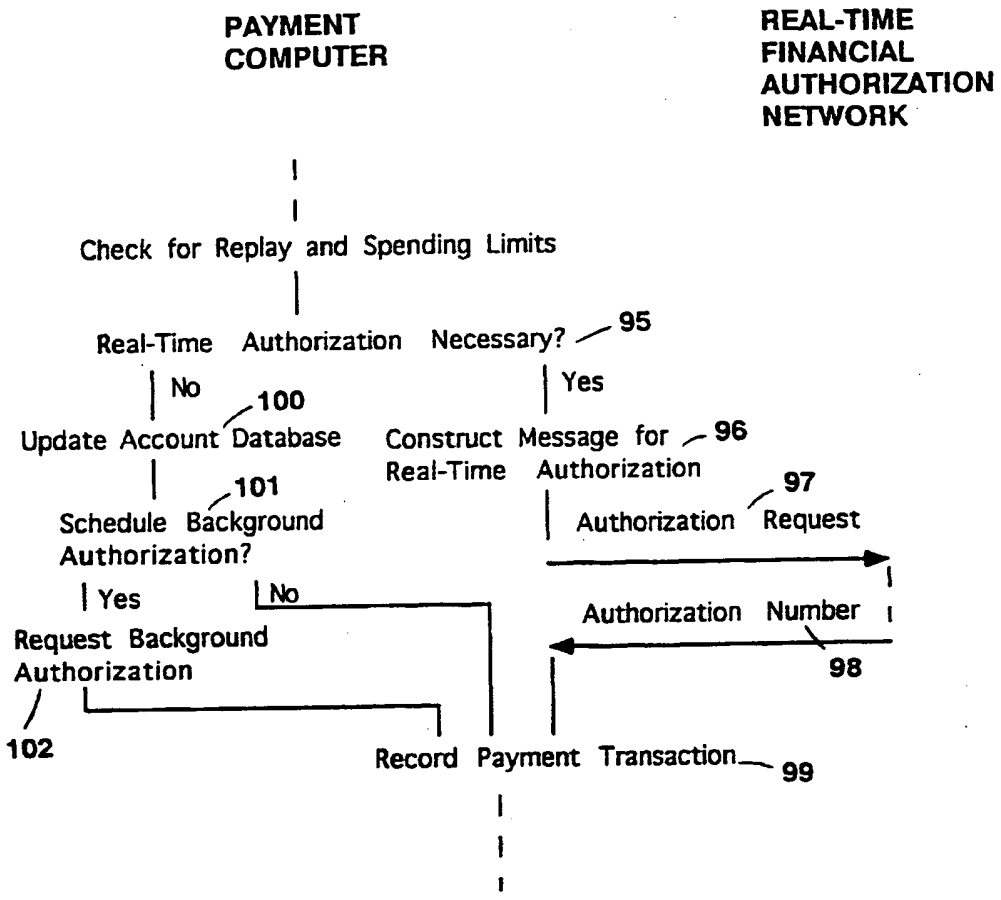
PAYMENT COMPUTER
REAL-TIME FINANCIAL AUTHORIZATION NETWORK
Check for Replay and Spending Limits
Real-Time Authorization Necessary?
95
No
Yes
100
Update Account Database
Construct Message for Real-Time Authorization
96
101
Schedule Background Authorization?
97
Authorization Request
Yes
No
Authorization Number
Request Background Authorization
98
102
Record Payment Transaction
99

FIG. 16